HERRERA PURDY LLP
Shawn M. Kennedy (SBN 218472)
skennedy@herrerapurdy.com
Andrew M. Purdy (SBN 261912)
apurdy@herrerapurdy.com
Bret D. Hembd (SBN 272826)
bhembd@herrerapurdy.com
4590 MacArthur Blvd., Suite 500
Newport Beach, CA 92660
Tel: (949) 936-0900
Fax: (855) 969-2050

HERRERA PURDY LLP
Nicomedes Sy Herrera (SBN 275332)
nherrera@herrerapurdy.com
Laura E. Seidl (SBN 269891)
lseidl@herrerapurdy.com
1300 Clay Street, Suite 600
Oakland, CA 94612
Tel: (510) 422-4700
Fax: (855) 969-2050

LIEFF CABRASER HEIMANN &
BERNSTEIN, LLP
Rachel Geman (*Pro Hac Vice*)
rgeman@lchb.com
Rhea Ghosh (*Pro Hac Vice*)
rghosh@lchb.com
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Tel: (212) 355-9500
Fax: (212) 355-9592

LIEFF CABRASER HEIMANN &
BERNSTEIN, LLP
Michael W. Sobol (SBN 194857)
msobol@lchb.com
Melissa Gardner (SBN 289096)
mgardner@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel: (415) 956-1000
Fax: (415) 956-1008

BURNS CHAREST LLP
Warren T. Burns (*Pro Hac Vice*)
wburns@burnscharest.com
Russell Herman (*Pro Hac Vice*)
rherman@burnscharest.com
900 Jackson Street, Suite 500
Dallas, TX 75202
Tel: (469) 904-4550
Fax: (469) 444-5002

BURNS CHAREST LLP
Christopher J. Cormier (*Pro Hac Vice*)
ccormier@burnscharest.com
4725 Wisconsin Avenue, NW, Suite 200
Washington, DC 20016
Tel: (202) 577-3977
Fax: (469) 444-5002

Interim Co-Lead Class Counsel

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

IN RE PLAID INC. PRIVACY
LITIGATION

THIS DOCUMENT RELATES TO:
ALL ACTIONS

Master Docket No.: 4:20-cv-03056-DMR

OPPOSITION TO PLAID'S MOTION TO DISMISS PLAINTIFFS' CONSOLIDATED AMENDED COMPLAINT

Hon. Donna M. Ryu

Action Filed: May 4, 2020

Trial Date: None Set

TABLE OF CONTENTS

Page

INTRODUCTION 1

FACTUAL BACKGROUND 2

I. Plaid's Wrongful And Deceptive Business Practices 2

II. Plaid Took Plaintiffs' Private Login And Banking Information 3

III. Plaintiffs Were Harmed By Plaid's Misconduct 4

ARGUMENT 5

I. Legal Standard 5

II. Plaid Acted Without Plaintiffs' Consent 5

A. Plaintiffs Were Not On Notice Of Plaid's Privacy Policy 6

B. Plaid's Privacy Policy Would Not Establish Consent If It Were Disclosed 8

III. Article III Is Satisfied 10

A. Plaid's Privacy Invasions Establish Injury In Fact 10

B. Plaid's Statutory Violations Establish Injury In Fact 11

C. Plaintiffs Have Standing To Seek Disgorgement Of Plaid's Unjustly-Earned Profits 13

D. Plaintiffs' Economic Injury Is Well-Pled 13

E. Plaintiffs' Injuries Are "Fairly Traceable" To Plaid's Conduct, And Redressable 15

IV. Plaintiffs' Claims Are Timely 16

V. Plaintiffs' Equitable Claims Are Not Barred By Remedies at Law 17

VI. Plaid's Rule 12(b)(6) Arguments Have No Merit 20

A. Plaintiffs Properly Plead Claims Under The California Constitution And For Common Law Invasion Of Privacy-Intrusion Into Private Affairs 20

B. Plaintiffs Have Properly Pleaded Claims Under The UCL 23

C. Plaintiffs Have Properly Pleaded Claims Under The CFAA And CDAFA 26

D. Plaintiffs Have Properly Pleaded A Claim Under The Stored Communications Act 35

E. Plaid's Violations Of The California Anti-Phishing Act Are Well-Pled 38

F. Plaintiffs Properly Plead A Claim For Deceit 42

G. Plaintiffs State A Claim For Unjust Enrichment/Quasi-Contract 44

CONCLUSION 45

TABLE OF AUTHORITIES

Page

CASES

Adams v. Johnston,
355 F.3d 1179 (9th Cir. 2004) 39

Adkins v. Comcast Corp.,
No. 16-05969, 2017 WL 3491973 (N.D. Cal. Aug. 1, 2017) 19

Am. Life Ins. Co. v. Stewart,
300 U.S. 203 (1937) 18

Applebaum v. Lyft, Inc.,
263 F. Supp. 3d 454 (S.D.N.Y. 2017) 7

Archer v. United Rentals, Inc.,
195 Cal. App. 4th 807 (2011) 23

Aryeh v. Canon Bus. Sols., Inc.,
55 Cal. 4th 1185 (2013) 16

Ashcroft v. Iqbal (2007),
556 U.S. 662 (2009) 5, 39

Astiana v. Hain Celestial Grp., Inc.,
783 F.3d 753 (9th Cir. 2015) 19, 44

Backhaut v. Apple, Inc.,
74 F. Supp. 3d 1033 (N.D. Cal. 2014) 36, 37

Bell Atlantic Corp. v. Twombly,
550 U.S. 554 (2007) 39

Beltran v. United States,
441 F.2d 954 (7th Cir. 1971) 14

Brazil v. Dole Packaged Foods, LLC,
660 F. App’x 531 (9th Cir. 2016) 44

Britton v. Girardi,
235 Cal. App. 4th 721 (2015) 17

Cahen v. Toyota Motor Corp.,
147 F. Supp. 3d 955, 971, 973 (N.D. Cal. 2015) 11

Cal. Bankers Ass’n v. Shultz,
416 U.S. 21 (1974) 20

Calsoft Labs, Inc. v. Panchumarthi,
No. 19 -04398-NC, 2020 WL 512123 (N.D. Cal. Jan. 31, 2020) 27

TABLE OF AUTHORITIES
(continued)

Page

Campbell v. Facebook,
77 F. Supp. 3d 836 (N.D. Cal. 2014).. 23

Campbell v. Facebook, Inc.,
951 F.3d 1106 (9th Cir. 2020) 11, 12, 16

Catholic League for Religious & Civil Rights v. City & Cnty. of San Francisco,
624 F.3d 1043 (9th Cir. 2010) 11

Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.,
20 Cal. 4th 163 (1999) 24

Central Bank & Trust v. Smith,
215 F. Supp. 3d 1226 (D. Wy. 2016)... 36, 38

Cline v. Reetz-Laiolo,
329 F. Supp. 3d 1000 (N.D. Cal. 2018)... 38

Colgate v. JUUL Labs, Inc.,
402 F. Supp. 3d 728 (N.D. Cal. 2019) 7

Creative Computing v. Getloaded.com, LLC,
386 F.3d 930 (9th Cir. 2004) 28

Daniel v. Ford Motor Co.,
806 F.3d 1217 (9th Cir. 2015) 26

Davis v. HSBC Bank Nevada,
691 F.3d 1152 (9th Cir. 2012) 24

Decoursey v. Sherwin-Williams Co.,
No. 19-02198, 2020 WL 1812266 (D. Kan. Apr. 9, 2020)... 36

Dinan v. SanDisk LLC,
No. 18-05420, 2020 WL 364277 (N.D. Cal. Jan. 22, 2020).. 8

eBay Inc. v. Digital Point Solutions, Inc.,
608 F. Supp. 2d 1156 (N.D. Cal. 2009)... 32

Ehling v. Monmouth-Ocean Hosp. Serv. Corp.,
961 F. Supp. 2d 659 (D.N.J. 2013)... 36

Erickson v. Pardus,
551 U.S. 89 (2007).. 5

Facebook, Inc. v. Fisher,
No. 09-05842, 2011 WL 250395 (N.D. Cal. Jan. 26, 2011).. 40

TABLE OF AUTHORITIES
(continued)

Page

Facebook, Inc. v. MaxBounty,
274 F.R.D. 279 (N.D. Cal. 2011).. 32

Facebook, Inc. v. Power Ventures, Inc.,
844 F.3d 1058 (9th Cir. 2016) 29

Facebook, Inc. v. Power Ventures, Inc.,
No. 08-05780, 2010 WL 3291750 (N.D. Cal. July 20, 2010) 27

Ferrington v. McAfee, Inc.,
No. 10-01455, 2010 WL 3910169 (N.D. Cal. Oct. 5, 2010) 43

Fidlar Techs. v. LPS Real Estate Data Sols., Inc.,
810 F.3d 1075 (7th Cir. 2016) 31, 32, 34

Flextronics Int'l, Ltd. v. Parametric Tech. Corp.,
No. 13-00034, 2014 WL 2213910 (N.D. Cal. May 28, 2014)... 35

Folgelstrom v. Lamps Plus, Inc.,
195 Cal. App. 4th 986 (2011) 22

Fox v. Ethicon Endo-Surgery, Inc.,
35 Cal. 4th 797 (2005)... 16

GM L.L.C. v. Autel.US Inc.,
No. 14-14864, 2016 WL 1223357 (E.D. Mich. Mar. 29, 2016).. 30

Gonzales v. Uber Techs., Inc.,
305 F. Supp. 3d 1078 (N.D. Cal. 2018)... 23, 28

Goodman v. HTC Am., Inc.,
No. 11-1793, 2012 WL 2412070 (W.D. Wash. June 26, 2012) 24

Greenwich Ins. Co, v. Media Breakaway,
No. 08-937, 2009 WL 6521581 (C.D. Cal. Jun. 11, 2009).. 41

Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.,
556 F. Supp. 2d 1122 (E.D. Cal. 2008) 32

Heeger v. Facebook, Inc.,
No. 18-06399, 2019 WL 7282477 (N.D. Cal. Dec. 27, 2019)... 22

Hernandez v. Hillsides, Inc.,
47 Cal. 4th 272 (2009).. 20, 21

Hexcel Corp. v. Ineos Polymers, Inc.,
681 F.3d 1055 (9th Cir. 2012) 17

TABLE OF AUTHORITIES
(continued)

Page

Hill v. NCAA,
7 Cal. 4th 1 (1994) 20

HiQ Labs, Inc. v. LinkedIn Corp.,
938 F.3d 985 (9th Cir. 2019) 27, 38

Hoffman v. 162 N. Wolfe LLC,
228 Cal. App. 4th 1178 (2014) 42, 43

In re Anthem Data Breach Litig.,
162 F. Supp. 3d 953 (N.D. Cal. 2016) 24

In re Apple & AT&TM Antitrust Litig.,
596 F. Supp. 2d 1288 (N.D. Cal. 2008) 28

In re Apple & ATTM Antitrust Litig,
No. 07-5152, 2010 WL 3521965 (N.D. Cal. July 8, 2010) 31

In re Facebook Privacy Litig.,
572 F. App'x 494 (9th Cir. 2014) 15

In re Facebook, Inc. Internet Tracking Litig.,
956 F.3d 589 (9th Cir. 2020) .... passim

In re Facebook, Inc. Sec. Litig.,
405 F. Supp. 3d 809 (N.D. Cal. 2019) 6

In re Facebook, Inc., Consumer Priv. User Profile Litig.,
402 F. Supp. 3d 767 (N.D. Cal. 2019) 9, 11, 15

In re Google Assistant Privacy Litig.,
457 F. Supp. 3d 797 (N.D. Cal. 2020) 8, 24

In re Google Inc. Cookie Placement Consumer Privacy Litig.,
806 F.3d 125 (3d Cir. 2015) 22

In re Google Referrer Header Privacy Litig.,
No. 10-04809, 2020 WL 3035796 (N.D. Cal. June 5, 2020) 5, 12, 13

In re Google, Inc. Privacy Policy Litig.,
No. 12-01382, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013) 15

In re iPhone Application Litig.,
844 F. Supp. 2d 1040 (N.D. Cal. 2012) 14, 22

In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.,
440 F. Supp. 3d 447 (D. Md. 2020) 15

TABLE OF AUTHORITIES
(continued)

Page

In re Tobacco II Cases,
46 Cal. 4th 298 (2009) 26

In re Toys R Us, Inc., Privacy Litig.,
No. 00-2746, 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001) 28

In re Vizio, Inc., Consumer Privacy Litig.,
238 F. Supp. 3d 1204 (C.D. Cal. 2017) 11, 22, 44

In re Webkinz Antitrust Litig.,
695 F. Supp. 2d 987 (N.D. Cal. 2010) 25

In re Zappos.com, Inc.,
888 F.3d 1020 (9th Cir. 2018) 14

Jewel v. Nat'l Sec. Agency,
673 F.3d 902 (9th Cir. 2011) 16

Johnson v. Riverside Healthcare Sys.,
534 F.3d 1116 (9th Cir. 2008) 39

Kasky v. Nike, Inc.,
27 Cal. 4th 939 (2002) 24

Katz v. Pershing LLC,
672 F.3d 64 (1st Cir. 2012) 14

Krottner v. Starbucks Corp.,
628 F.3d 1139 (9th Cir. 2010) 14

Kwikset Corp. v. Superior Ct.,
51 Cal. 4th 310 (2011) 23

Low v. LinkedIn Corp.,
900 F. Supp. 2d 1010 (N.D. Cal. 2012) 22

LSH CO v. Transamerica Life Ins. Co.,
No. 18-09711, 2019 WL 3064422 (C.D. Cal. Mar. 20, 2019) 17

Luong v. Subaru of Am., Inc.,
No. 17-03160, 2018 WL 2047646 (N.D. Cal. May 2, 2018) 19

Mangum v. Action Collection Serv., Inc.,
575 F.3d 935 (9th Cir. 2009) 16

Marolda v. Symantec Corp.,
672 F. Supp. 2d 992 (N.D. Cal. 2009) 44

TABLE OF AUTHORITIES
(continued)

Page

Matera v. Google, Inc.,
No. 15-4062, 2016 WL 5339806 (N.D. Cal. Sept. 23, 2016). 12

McDonald v. Coldwell Banker,
543 F.3d 498 (9th Cir. 2008) 25

McKee v. Audible, Inc.,
No. 17-1941, 2017 WL 4685039 (C.D. Cal. July 17, 2017).......... 7

McLellan v. Fitbit, Inc.,
No. 16-00036, 2018 WL 2688781 (N.D. Cal. June 5, 2018).......... 44

Microsoft Corp. v. Doe,
No. 14-00811, 2015 WL 4937441 (E.D. Va. Aug. 17, 2015) 30

Microsoft Corp. v. Mutairi,
No. 14-00987, 2015 U.S. Dist. LEXIS 95541 (D. Nev. June 25, 2015).......... 30

Mobile Active Def., Inc. v. L.A. Unified Sch. Dist.,
No. 15-8762, 2016 WL 7444876 (C.D. Cal. Apr. 6, 2016).......... 33

Moss v. U.S. Secret Serv.,
572 F.3d 962 (9th Cir. 2009) 45

Multiven, Inc. v. Cisco Sys., Inc.,
725 F. Supp. 2d 887 (N.D. Cal. July 20, 2010) 29

NACM Tampa, Inc. v. Sunray Notices, Inc.,
No. 15-1776, 2017 WL 2209970 (M.D. Fla. Feb. 8, 2017).......... 34

NetApp v. Nimble Storage, Inc.,
No. 13-05058, 2015 WL 400251 (N.D. Cal. Jan. 29, 2015).......... 31

NetApp, Inc. v. Nimble Storage,
41 F. Supp. 3d 816 (N.D. Cal. 2014).......... 32

Neubronner v. Milken,
6 F.3d 666 (9th Cir.1993) 5

Nguyen v. Barnes & Noble Inc.,
763 F.3d 1171 (9th Cir. 2014) 6, 7

Opperman v. Path, Inc.,
205 F. Supp. 3d 1064 (N.D. Cal. 2016).......... 8, 10, 20, 22

Oracle Am., Inc. v. TERiX Comput. Co.,
No. 13-03385, 2014 WL 31344 (N.D. Cal. Jan. 3, 2014).......... 34

TABLE OF AUTHORITIES
(continued)

Page

Overton v. Bird Brain, Inc.,
No. 11-1054, 2012 WL 909295 (C.D. Cal. Mar. 15, 2012)................ 44

Patel v. Facebook, Inc.,
932 F.3d 1264 (9th Cir. 2019) 21

Philips v. Ford Motor Co.,
No. 14-02989, 2015 WL 4111448 (N.D. Cal. July 7, 2015) 19

Pineda v. Williams-Sonoma Stores, Inc.,
51 Cal. 4th 524 (2011) 41

Riley v. California,
573 U.S. 373 (2014)................ 21

Romero v. Securus Techs., Inc.,
216 F. Supp. 3d 1078 (S.D. Cal. 2016)................ 23

Satmodo, LLC v. Whenever Commcns.., LLC,
No. 17-0192, 2017 WL 6327132 (S.D. Cal. Dec. 8, 2017) 29, 31

Shroyer v. New Cingular Wireless Servs., Inc.,
622 F.3d 1035 (9th Cir. 2010) 5

Shurgard Storage Centers, Inc., v. Safeguard Self Storage, Inc.,
119 F. Supp. 2d 1121 (W.D. Wash. 2000)................ 29, 32

Singer Co. v. Superior Court,
179 Cal. App. 3d 875 (1986) 14

Sloan v. GM, LLC,
287 F. Supp. 3d 840 (N.D. Cal. 2018)................ 43

Sonner v. Premier Nutrition Corp.,
971 F.3d 834 (9th Cir. 2020) 18, 19

Spokeo, Inc. v. Robins,
136 S. Ct. 1540 (2016)................ 10, 11, 12

State v. Mayze,
622 S.E.2d 836 (Ga. 2005) 15

Steel Co. v. Citizens for a Better Env't,
523 U.S. 83 (1998)................ 15

Svenson v. Google Inc.,
No. 13-04080, 2016 WL 8943301 (N.D. Cal. Dec. 21, 2016)................ 15

TABLE OF AUTHORITIES
(continued)

Page

T. K. v. Adobe Sys. Inc.,
No. 17-04595, 2018 WL 1812200 (N.D. Cal. Apr. 17, 2018) 18

Theofel v. Farey-Jones,
359 F.3d 1066 (9th Cir. 2004) 37

Therapeutic Research Faculty v. NBTY, Inc.,
488 F. Supp. 2d 991 (E.D. Cal. 2007) 29

Thompson v. Transamerica Life Ins. Co.,
No. 18-05422, 2018 WL 6790561 (C.D. Cal. Dec. 26, 2018) 19

Ticketmaster L.L.C. v. Prestige Entm't W., Inc.,
315 F. Supp. 3d 1147 (C.D. Cal. 2018) 31

T-Mobile USA, Inc. v. Terry,
862 F. Supp. 2d 1121 (W.D. Wash. 2012) 34

Trazo v. Nestle USA, Inc.,
113 F. Supp. 3d 1047 (N.D. Cal. 2015) 44

United States v. Corinthian Colls.,
655 F.3d 984 (9th Cir. 2011) 5

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) 20

United States v. Neville,
985 F.2d 992 (9th Cir. 1993) 40

United States v. Nosal,
844 F.3d 1024 (9th Cir. 2016) 27

United States v. Weaver,
636 F. Supp. 2d 769 (C.D. Ill. 2009) 38

United States v. Yücel,
97 F. Supp. 3d 413 (S.D.N.Y. 2015) 30, 31

Van Patten v. Vertical Fitness Grp., LLC,
847 F.3d 1037 (9th Cir. 2017) 10, 12

Wildin v. FCA US LLC,
No. 17-02594, 2018 WL 3032986 (S.D. Cal. June 19, 2018) 19

Wilding v. DNC Servs.,
No. 16-61511, 2017 WL 6345492 (S.D. Fla. Aug. 25, 2017) 14

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

12 U.S.C. § 3401 12

18 U.S.C. § 1030 .... passim

18 U.S.C. § 1030(a)(4) 32

18 U.S.C. § 1030(a)(5)(A) 34

18 U.S.C. § 1030(a)(6) 32

18 U.S.C. § 1030(c)(4)(A)(i)(I) 27

18 U.S.C. § 1030(e)(11) 30

18 U.S.C. § 1030(g) 16, 27

18 U.S.C. § 2510(12) 36

18 U.S.C. § 2510(12)(D) 37

18 U.S.C. § 2510(15) 36

18 U.S.C. § 2510(17)(B) 37

18 U.S.C. § 2701 .... passim

18 U.S.C. § 2701(a) 35

18 U.S.C. § 2701(a)(1) 36

18 U.S.C. § 2707 35

18 U.S.C. § 2707(f) 16

18 U.S.C. § 2711(1) 36

Cal. Bus. & Prof. Code § 17203 26

Cal. Bus. & Prof. Code § 22577 .... 24, 25

Cal. Bus. & Prof. Code § 22948 12

Cal. Bus. & Prof. Code § 22948.2 .... 39, 40, 41

Cal. Bus. & Prof. Code § 22948.3 41

Cal. Bus. & Prof. Code § 22948.3(a)(2) 40

Cal. Bus. & Prof. Code § 22948.3(d) 41

TABLE OF AUTHORITIES
(continued)

Page

Cal. Civ. Code § 1709 .... 23, 42, 43, 44

Cal. Fin. Code § 4051 24

Cal. Pen. Code § 502 .... passim

Cal. Pen. Code § 502(a) 12

Cal. Pen. Code § 502(b)(10) 34, 35

Cal. Pen. Code § 502(c)(1) 31

Cal. Pen. Code § 502(c)(4) 31

Cal. Pen. Code § 502(c)(8) 34

Cal. Pen. Code § 502(e)(1) 27, 28

REGULATIONS

16 C.F.R. § 313.3(b)(1)-(2) 7

16 C.F.R. § 313.4 8

16 C.F.R. § 313.5 8

RULES

Fed. R. Civ. P. 57 17

Fed. R. Civ. P. 57 1937 Advisory Committee Notes 17

Fed. R. Civ. P. 9(b) 5

OTHER AUTHORITIES

Camille Calman, *Bigger Phish to Fry: California's Anti-Phishing Statute and Its Potential Imposition of Secondary Liability on Internet Service Providers*, 13 Rich. J.L. & Tech. 2 (2006) 40

S. Rep. 104-357 (1996) 11

S. Rep. 99-432 (1986) 11

S. Rep. No. 99-541 (1986) 11

Vasileios Karagiannopoulos, *From Morris to Nosal: The History of Exceeding Authorization and the Need for a Change*, 30 J. Marshall J. Info. Tech. & Privacy L. 465 (2014) 11

INTRODUCTION

The Consolidated Amended Complaint (Dkt. 61) ("CAC") describes in detail how Plaid embeds its own software in Venmo and other apps to surreptitiously collect private bank login information—and then actual bank account transactions—from Plaintiffs and millions of other consumers. This egregious invasion of privacy is facilitated (and exacerbated) by Plaid's pretending to be consumers' trusted banks, and otherwise hiding the true nature of its misconduct. Plaintiffs neither knew about nor consented to Plaid's systematic monitoring of their personal financial lives, or to Plaid's collection and use of Plaintiffs' data. The well-pleaded allegations state claims under multiple federal and state laws. In its Motion to Dismiss (Dkt. 78) ("MTD"), Plaid paints itself as a harmless conduit that Plaintiffs used to connect apps to Plaintiffs' financial accounts, ignoring the allegations and injecting fact-based defenses that will require discovery. Its motion should be denied.

First, Plaid entirely fails to demonstrate its principal argument that Plaintiffs consented to its activities. Plaid's express design from the start was that consumers would not learn Plaid even exists. Plaid's inadequate and obscure privacy policy failed to provide actual or constructive notice of Plaid's activities. Consent is not a defense to any, let alone all, of Plaintiffs' claims.

Second, Plaintiffs adequately allege standing. Privacy invasions are concrete and redressable, the statutes under which Plaintiffs seek relief provide additional statutory standing, and recent governing law confirms the existence of Plaintiffs' injuries (including economic harm).

Third, Plaintiffs' claims are timely because they allege misconduct within the statutes of limitations of their claims (namely, Plaid's access, continuous collection, and use of private data). In any event, application of the discovery rule and Plaid's fraudulent concealment of its conduct would save any claims that otherwise would be untimely (although there are none).

Fourth, Plaintiffs adequately allege all the specific elements of their claims and entitlement to the prayed-for relief. Plaid's 12(b)(6) arguments boil down to constant reiteration of its failed consent argument, premature disagreements over the facts, and an unsupported challenge to whether it is subject to privacy-related statutes. Yet, Plaid's intrusion into consumers' private lives is exactly what contemporary statutes—drawing on centuries of common-law principles—proscribe.

FACTUAL BACKGROUND

I. Plaid's Wrongful And Deceptive Business Practices

Plaid's business operates as follows: ***First***, Plaid embeds software in the apps of financial technology (fintech) clients that enable funds transfers, such as Venmo, Coinbase, Square's "Cash App," and Stripe (the "Apps"). ¶ 31.[1] When consumers are prompted to link or verify their bank account for these Apps, Plaid's software activates. ¶¶ 31-32. Plaid designed its software to mimic a standard "OAuth" login procedure (that is, one where a website or app user is redirected to log in directly to a third-party website), including by mimicking the bank's mobile website. ¶ 38. Specifically, Plaid presents the consumer with an interface that appears to come from their bank, including the bank's logo and color scheme. *Id.* The experience—a shift in the screen, suggesting the user has been directed from the app to the bank— gives the definite impression that login information is being passed directly to trusted financial institutions. *Id.* Plaid provides no warnings that reasonable consumers would expect when requested to hand over their bank login credentials to a third-party instead. Plaid makes no effort to meaningfully disclose what it is about to do and obtain consent. Instead, Plaid hides the link to its (substantively inadequate) privacy policy, *via* disproportionately small font and a light gray color designed to escape attention. ¶¶ 67-69. The design features of Plaid's software look like familiar banking pages to consumers, inducing them to enter private credentials to "log in" to the bank. ¶¶ 35, 37-41. In reality, consumers unwittingly hand their credentials directly to Plaid. ¶¶ 35, 45.

Second, Plaid takes the consumer's login credentials and uses them to establish its own connection to the bank. ¶¶ 45, 70. Once that connection is established, Plaid accesses the bank's computer systems for all available data connected to that consumer, including years of historical transaction data, identifying information, and data related to all associated savings, investment, and accounts—even minor children's accounts. ¶¶ 5, 49-50, 53, 56. Plaid continues to collect that data every few hours, regardless of whether the data has any tie to the App's money-transfer purposes, and regardless of whether the consumer stops using or deletes that App. ¶¶ 5, 55, 267.

Third, having scraped all available data, Plaid exports the data wholesale to its own servers,

[1] Throughout this brief, all citations identified with "¶" are to paragraphs of the CAC.

where it cross-references it with other data ("enriches" it). ¶¶ 54-55. Plaid then sells products that make the data available to its clients, the Apps. ¶ 59. Plaid employs a large team of data scientists to run analytics on the data so that it can develop value-added products, which it also sells. ¶¶ 63-64.

Plaid has collected consumer banking data from over 200 million individual accounts, what it touts as "one of the largest transactional data sets in the world." ¶¶ 28, 54, 57. This is remarkable given—indeed, because—Plaid's objective was that "most people will never know we exist." ¶ 76.

II. Plaid Took Plaintiffs' Private Login And Banking Information

Contrary to Plaid's suggestion, Plaintiffs specifically, expressly, and repeatedly allege that Plaid's software was used to connect the Apps to their respective bank accounts. ¶ 99 (Plaintiffs are "App users ***who linked their financial accounts using Plaid's software*** integrated with the app") (emphasis added); ¶ 215 ("Plaid deceptively acquired [Plaintiffs'] bank login credentials and informed their financial institutions that they had provided Plaid with permission to gain access to all information available in their bank accounts"). The individual Plaintiffs believed, at the time, that they were logging into their own banks (¶¶102, 113, 123, 132, 142, 152, 161, 170, 180, 191, 201), and describe how their bank accounts were actually accessed by Plaid through the process illustrated in the CAC. For example, Plaintiff Anderson alleges that, when she signed up to use Venmo and Cash App, she was prompted in those apps to connect her bank account by logging into it, and that she actually did so. ¶¶ 100, 102-05. Similarly, Ms. Anderson alleges that, to the extent she recalls specific details regarding the process of logging into her bank account in the apps, those details are "consistent with the discussion of Plaid's interface" in the CAC. ¶ 101. She also alleges that her financial account was "linked" to and "verified for use with" Venmo and Cash App. ¶ 109. Each of the named Plaintiffs makes a similar allegation. ¶¶ 109, 119, 129, 139, 149, 158, 167, 177, 187, 198, 207.[2]

Lest there be any doubt (and there is not), Plaintiffs' allegations *necessarily* refer to Plaintiffs linking their accounts through Plaid's instant verification and linking process, through which consumers

[2] And, behind the scenes, Plaid's software operated in materially the same way for each Plaintiff in that it followed the same process of surreptitiously collecting their bank login credentials while hiding Plaid's role and indicating that Plaid was and/or represented the banks. While certain of the named Plaintiffs first connected Apps to their bank accounts using versions of Plaid's software from prior to 2016 and others from after Plaid implemented its "Managed OAuth" procedure (*see* ¶¶ 34-35, 121, 140, 150, 159, 188, 199), in all cases Plaid received and maintained login information through deception.

are directed to log into their bank accounts using Plaid's spoofed bank login screens. ¶¶ 32-41. The CAC explains that the *sole alternative* to link a bank account is a different process involving micro-deposits to a consumer's account, where consumers must report the amounts back to the App. ¶ 32. None of the Plaintiffs allege they engaged in micro-deposit verification, which would *not* be consistent with Plaid's interface. Instead, all allege facts consistent with Plaid's process of instant verification.

Plaintiffs further allege that Plaid actually took their private data from their bank accounts, further confirming their allegations that, unknowingly at the time, they were using Plaid's software. For example, Plaintiffs allege that Plaid (1) "obtained access to their personal financial accounts and stripped out all available data" (¶ 208); (2) "intruded upon Plaintiffs' . . . private affairs and concerns by improperly accessing, downloading, transferring, selling, storing and using their private banking information" (¶ 262); and (3) "removed Plaintiffs' . . . banking data from the secure banking environment, selling or transferring it to the [] Apps and storing it for its own use." ¶ 292(a). In addition, certain Plaintiffs allege that, as a result of having connected the Apps to their bank accounts through Plaid, Plaid accessed their minor children's accounts without authorization. ¶¶ 110, 120. Plaid's suggestion that Plaintiffs failed to allege their connection to Plaid is easily belied by the CAC.

III. <u>Plaintiffs Were Harmed By Plaid's Misconduct</u>

Plaid intruded upon a deeply personal aspect of Plaintiffs' lives. Banking information is private, not only because it reveals sensitive facts about people's income and expenditures, but because it is a sharp light on the details of their lives, priorities, habits, and associations. ¶¶ 50, 208. What Plaid took from Plaintiffs' accounts is particularly illuminating, in that it includes stored technical information about the precise locations where Plaintiffs made their purchases, as well as data from other accounts. ¶¶ 27, 208. In Plaid's control, this data becomes even more revealing: Plaid acknowledges that it runs "analytics" and draws inferences about those whose accounts it has accessed, beyond what may be shown by isolated data points. ¶¶ 25, 64. Plaid's privacy invasions and abuse of the trust that Plaintiffs placed in their own financial institutions (by representing itself as those institutions) violates social norms and Plaintiffs' dignitary rights to control access to their own information, and to decide for themselves what, when, and why it should be shared. Plaid parries that it does not "sell" Plaintiffs' data, but it is beyond dispute that Plaid, at a minimum, sells products that make Plaintiffs' data available to others (¶¶ 99, 206, 208-11, 214-34) and used Plaintiffs' data to generate value for itself. ¶¶ 63-65, 107.

The harm to Plaintiffs' privacy and dignitary interests is pronounced, and gives rise to Plaintiffs' entitlement to seek disgorgement of the benefits Plaid has acquired by virtue of these abuses. Plaid's misconduct also caused Plaintiffs to lose indemnification rights and protections their data would otherwise have had (¶¶ 47, 78, 215-24, 335), and lose control over their own sensitive financial information—property of demonstrable value (¶¶ 6, 59, 62, 228-31). Plaintiffs now face a heightened risk of identity theft and fraud, which has required expenditures of time and resources. ¶¶ 57, 79, 201, 108, 118, 206, 232-35.

ARGUMENT

I. Legal Standard

On a Rule 12(b)(6) motion, the court must "accept as true all of the factual allegations contained in the complaint," *Erickson v. Pardus*, 551 U.S. 89, 94 (2007), and construe them "in the light most favorable to the [Plaintiffs]." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). A claim may be dismissed "only where there is no cognizable legal theory" or the complaint does not plead sufficient facts to "state a facially plausible claim to relief." *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1041 (9th Cir. 2010) (citations omitted). A claim is facially plausible when the facts alleged allow the court to "draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Likewise, when considering challenges to Article III standing pursuant to Rule 12(b)(1), the Court should construe Plaintiffs' allegations as true. *In re Google Referrer Header Privacy Litig.*, No. 10-04809, 2020 WL 3035796, at *3-4 (N.D. Cal. June 5, 2020). As to Rule 9(b), the pleading standard "requires only that the circumstances of fraud be stated with particularity." *United States v. Corinthian Colls.*, 655 F.3d 984, 992 (9th Cir. 2011). "Malice, intent, knowledge, and other conditions of a person's mind may be alleged generally." Fed. R. Civ. P. 9(b). Further, the Rule 9(b) standard may be relaxed when fraud allegations relate to matters particularly within the opposing party's knowledge, such that a plaintiff cannot be expected to have personal knowledge. *See Neubronner v. Milken*, 6 F.3d 666, 672 (9th Cir.1993).

II. Plaid Acted Without Plaintiffs' Consent

Plaintiffs allege they did not consent to Plaid's initial acquisition of their account credentials or subsequent access to and use of their banking information. ¶¶ 1, 3, 32, 76, 107, 117, 127, 137, 147, 156, 165, 175, 185, 196, 205, 208, 226, 265, 315, 331, 346. Yet Plaid asserts consent as an overarching defense to all of Plaintiffs' claims, purportedly based upon the existence and terms of its privacy policy. *See* MTD at 1, 3-5, 13, 16, 18, 27, 31-36. Plaid's consent defense fails for multiple, independently-sufficient reasons: (1) Plaid's privacy policy is unenforceable; (2) even if it applied, it is inadequate to establish knowing consent to Plaid's conduct alleged; and (3) Plaid has failed to support its argument with evidence that would be properly before the Court on this motion.[3]

A. **Plaintiffs Were Not On Notice Of Plaid's Privacy Policy**

Plaid cannot and does not claim that Plaintiffs actually saw its privacy policy or manifested agreement to its terms. A consumer cannot be bound by the terms of an online privacy policy unless—at a minimum, among other requirements—those terms are so conspicuously displayed to put the consumer on constructive notice of them. *See Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1178–79 (9th Cir. 2014) ("[T]he onus must be on website owners to put users on notice of the terms to which they wish to bind consumers.").

Here, Plaid operated in the deep background, soliciting bank login information through a "familiar[]" process that gave the false impression that only trusted apps and banks were involved in the account linking process. ¶ 41. To any reasonable consumer, it appeared that the App, not a third-party, was linking their accounts to banks.[4] ¶¶ 35-45. In Plaid's process, it was never apparent that a data aggregator was even present. *Id*. The law does not bind consumers to a purported contract of whose existence the consumers were unaware, with a company of whose existence consumers are unaware, let alone a contract granting that company unrestricted access to the sensitive information in consumer's

[3] Plaid seeks judicial notice of documents to support its consent-based arguments, but the policies it cites are facially irrelevant to the issue of Plaintiffs' knowledge and consent. This is because the policies Plaid submitted were not in place at the various relevant dates when Plaid first accessed Plaintiffs' information, including in March and June 2014, April and August 2015, July 2016, and January 2019. ¶¶ 100, 111, 121, 130, 140, 150, 159, 168, 178, 188, 199. This alone provides sufficient basis to deny Plaid's motion on the issue of consent. *See In re Facebook, Inc. Sec. Litig.*, 405 F. Supp. 3d 809, 831 (N.D. Cal. 2019) ("[J]udicial notice on the issue of user consent is not appropriate.") (citation omitted); *see also* Plaintiffs' Opp. to Request for Judicial Notice, filed herewith.

[4] Venmo users were presented with a screen stating "Venmo uses Plaid," but the screen did not explain that Plaid is a third-party independent of Venmo, rather than a service of Venmo, or the banks. ¶¶ 67-68. Worse, some Apps make no Plaid-related consumer disclosures whatsoever through Plaid's interface, simply directing consumers to screens that appear to come from their banks. ¶ 66.

bank accounts.[5] "[C]ontracts cannot be formed on the basis of stealth drafting." *Colgate v. JUUL Labs, Inc.*, 402 F. Supp. 3d 728, 763 (N.D. Cal. 2019); *see also McKee v. Audible, Inc.*, No. 17-1941, 2017 WL 4685039, at *10-11 (C.D. Cal. July 17, 2017) ("It is simply hard for the Court to imagine that a reasonable consumer registering the Amazon Echo expects to be presented with terms of use governing his or her contractual relationship with separate corporate entities, *let alone one he or she has never dealt with*. . . . [n]o amount of hyperlinking . . . changes the reality of internet commerce: a consumer agreeing to terms of use for his or her Echo cannot be reasonably expected to know they are giving up the right to sue Audible."). These principles apply in particular in the context of private financial information, in light of (among other sources) the heightened disclosure requirements under the Gramm-Leach-Bliley Act ("GLBA"). 16 C.F.R. § 313.3(b)(1)-(2) (requiring clear and conspicuous policies on which consumers have actual and acknowledged notice).

Contrary to applicable law, Plaid failed to provide reasonable notice of the terms of its privacy policy. Instead, Plaid effectively hid those terms, including by de-emphasizing the subtle hyperlink to its privacy policy, which was not underlined or offset to give any indication that it was a hyperlink, and used light grey font and a miniscule font size much smaller than other large, colorful, high-contrast items on the screen. The hyperlink is difficult to see in the large screenshot within Plaintiffs' CAC, let alone on a mobile device, and there is no checkbox to assent to it, ensuring that it would be, and was, overlooked. ¶¶ 67-69. "Given the breadth of the range of technological savvy of online purchasers, consumers cannot be expected to ferret out hyperlinks to terms and conditions to which they have no reason to suspect they will be bound." *Nguyen*, 763 F.3d at 1179.

Even in disputes over the applicability of terms between *known* parties where the nature of the interaction is clear, courts consistently have found that similarly inadequate notice rendered purported contracts unenforceable. *See, e.g.*, *Colgate*, 402 F. Supp. 3d at 764 (no consent by website visitors where non-underlined hyperlink near "sign up" button was "not a different color, underlined, italicized, or in any way visually distinct from the surrounding text"); *Applebaum v. Lyft, Inc.*, 263 F. Supp. 3d 454, 467 (S.D.N.Y. 2017) (no consent by Lyft drivers where hyperlink was a different color but "there were no

[5] Banking information is subject to particularly exacting, historically recognized, privacy protections. *See infra* Arg. § VI-A.

familiar indicia to inform consumers that there was in fact a hyperlink that should be clicked and that a contract should be reviewed"). Plaid has not come close to complying with the law.

B. Plaid's Privacy Policy Would Not Establish Consent If It Were Disclosed

Even if Plaintiffs were on constructive notice of Plaid's privacy policy, Plaid could not establish consent to its specific conduct. The generic terms of Plaid's hidden policy do not explain what Plaid actually is, or does. Where a privacy policy is asserted as a defense, courts examine whether "a reasonable user reading the privacy policy must have understood it to cover" the conduct at issue. *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 823 (N.D. Cal. 2020); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072–73 (N.D. Cal. 2016) ("[C]onsent is only effective if the person alleging harm consented 'to the particular conduct, or to substantially the same conduct'" and if the alleged tortfeasor did not exceed the scope of that consent.") (citation omitted). Plaid's vague and overly-general privacy policy fails this standard. And in any case, the reasonable consumer standard "raises questions of fact that are appropriate for resolution on a motion to dismiss only in rare situations." *Dinan v. SanDisk LLC*, No. 18-05420, 2020 WL 364277, at *7 (N.D. Cal. Jan. 22, 2020) (citation omitted).

Plaid highlights and re-emphasizes out-of-context snippets from the policy in a chart, but ignores Plaintiffs' allegations about the misleading and deceptive nature of the privacy policy on the whole. ¶¶ 71, 74-76. Neither has Plaid established that its policy "accurately reflects" its practices, as required under the GLBA. 16 C.F.R. §§ 313.4 & 313.5. The specific and prominent disclosures a reasonable consumer would expect from a company acquiring access to their extremely private and sensitive bank account data are nowhere found in Plaid's generic policy. Here, a reasonable App user viewing the policy would not understand that *their* private banking credentials and financial data were even at issue.

The policy strongly, and deceptively, suggests that App users' banking data would *not* be accessed by Plaid. To start, the policy states that Plaid collects consumers' banking login information only when they connect their accounts "through Plaid"—something consumers interacting with Apps and bank login screens would be unaware was happening.[6] Even that data collection, the policy says,

[6] This reasonable inference is bolstered by another provision in Plaid's current privacy policy, which states that Plaid obtains information when consumers "connect to our services through a developer's application" about "**which features** within our services you access." Dettmer Decl. Ex. A, at 4 (emphasis added). The typical experience of an App user does not permit them to choose from any Plaid

occurs "where applicable" (*id.* at 2), suggesting some frequency far lower than Plaid's actual practice of transmitting all consumer login information to itself, at all times. If, despite implicit and explicit suggestions to the contrary, a Plaintiff had surmised that Plaid's policy might apply to the account connections they were making, they would still understand that they fell within the exception where any collection of their login credentials was not "applicable" based on the more prominent statement in the Apps that their "credentials will never be made accessible to" the App that used Plaid (¶¶ 67-68, 360). If a consumer realized Plaid had accessed their accounts at all, they would also reasonably expect that disconnecting their accounts from the App would terminate Plaid's access (*see* MTD at 6, asserting that consumers are told they can "turn off Venmo's use of Plaid"), but disconnecting bank accounts from *Venmo* does not disconnect them from Plaid, or cause Plaid to delete the data it already has. ¶ 55.

Furthermore, consistent with any common sense expectation where private banking data is concerned, the policy can fairly be read to state that Plaid's access to account data would have some relationship to the function of the App to which financial accounts are being linked: "The information we receive from the financial product and service providers that maintain your financial accounts [*i.e.*, banks] **varies depending on the specific Plaid services developers use to power their applications**, as well as the information made available by those providers." Dettmer Decl. Ex. A, at 2-3 (emphasis added). Because the Apps' function of transferring funds has nothing to do with historical banking data, address information, or the other private data beyond confirming that a consumer owns the linked account, it is reasonable to expect that any "Plaid services" used by the Apps would not collect any data beyond that needed to verify the account. This reasonable interpretation is further bolstered by the policy's statement that it collects EU citizens' data "to fulfill [Plaid's] responsibilities and obligations" to consumers; and that it retains such information "for no longer than necessary to fulfill the purposes for which it was collected and used." This policy does not reasonably disclose that Plaid collects banking data without reference to the "purpose" of the particular App at issue.[7]

"features," so this reference suggests that connecting "through Plaid" is a different process.

[7] No part of Plaid's privacy policy mentions that Plaid is a data aggregator that will retain users' banking credentials; use them on an indefinite, ongoing basis to acquire forward- and backward-looking private data about their purchases; or use and sell that and other data for its own benefit. *See In re Facebook, Inc., Consumer Priv. User Profile Litig.* ("*Facebook Consumer Privacy*"), 402 F. Supp. 3d 767, 792 (N.D. Cal. 2019) (rejecting argument based on consent where policy did "not come close to disclosing

Plaintiffs' interpretation is supported by material factual allegations, including that banks and industry groups recognized the "lack of clarity and transparency" provided by data aggregators such as Plaid regarding its collection and use of private data "isn't fair or right." ¶¶ 78, 80-81; *see also* ¶ 79 ("consumers are not given adequate information or control over what information is being taken, how long it is accessible, and how it will be used in the future."). Plaid's contrary interpretation of its privacy policy should be rejected on this motion. *See Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011) (if two alternative plausible explanations exist, the plaintiff's version should be followed at the motion to dismiss stage). Plaid's argument that Plaintiffs show "consent" by not alleging they asked Plaid to delete their data (which Plaid asserts, without support, it would do upon request) is contradicted by Plaintiffs' specific request for an order requiring Plaid to purge the data it has unlawfully collected. MTD at 7, 13; Prayer for Relief D. At most, factual disputes about consent remain, and "[t]his is an issue for the jury." *Opperman*, 205 F. Supp. 3d at 1073.

III. Article III Is Satisfied

Plaid acquired Plaintiffs' banking credentials in violation of established common law and statutory protections, without consent, and used that private information to enrich itself. These allegations satisfy standing, as shown below.

A. Plaid's Privacy Invasions Establish Injury In Fact

Plaintiffs have standing to bring all claims asserted in this action because each relates to Plaid's invasion of their privacy rights. Such violations constitute "concrete and particularized injury" for purposes of Article III. *See Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) ("Actions to remedy defendants' invasions of privacy . . . have long been heard by American courts"). "It is beyond meaningful dispute that a plaintiff alleging invasion of privacy . . . presents a dispute the Court is permitted to adjudicate." *Opperman*, 87 F. Supp. 3d at 1057.

Contrary to Plaid's incorrect suggestion, intangible injuries may be "concrete" and constitute injury in fact. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). "To say that a 'mere' privacy invasion is not capable of inflicting an 'actual injury' serious enough to warrant the attention of the

the massive information-sharing program" at issue).

federal courts is to disregard the importance of privacy in our society, not to mention the historic role of the federal judiciary in protecting it." *Facebook Consumer Privacy*, 402 F. Supp. 3d at 786 (citation omitted) (privacy injury sufficient for SCA, California common law intrusion into private affairs, constitutional right to privacy, negligence, deceit by concealment, breach of implied covenant of good faith and fair dealing, unjust enrichment, and UCL claims, among others). Plaid relies on an inapposite case, *Cahen v. Toyota Motor Corp.*, wherein the cursory assertion, without support, that the Constitution protected data about a vehicle's driving history, performance, and occasional location, did not pass muster. 147 F. Supp. 3d 955, 971, 973 (N.D. Cal. 2015), *aff'd*, 717 F. App'x 720 (9th Cir. 2017). By contrast, here, the manner, circumstances, and nature of Plaid's privacy violations are alleged in detail, and sensitive, protected information is at issue. Facts §§ I-III.

Plaid disputes Plaintiffs' standing by claiming that Plaintiffs consented to or were informed of (and failed to attempt to stop) Plaid's practices. MTD at 13 (restating consent defense in another guise). But its argument "improperly conflates the merits of Plaintiffs' claims with their standing to bring suit." *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1216 (C.D. Cal. 2017). The "standing analysis . . . [may not] be used to disguise merits analysis, which determines whether a claim is one for which relief can be granted if factually true." *Catholic League for Religious & Civil Rights v. City & Cnty. of San Francisco*, 624 F.3d 1043, 1049 (9th Cir. 2010). Recently, as Judge Chhabria noted in *Facebook Consumer Privacy*, "in virtually every privacy case, consent will be part of the merits inquiry. Because courts presume success on the merits when evaluating standing, ***these are not standing issues in privacy cases***." 402 F. Supp. 3d at 788 (emphasis added); *see also Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1119 n.9 (9th Cir. 2020) (argument that Plaintiffs consented to the use of URL data was a "merits arguments in disguise" that "tell[s] us nothing about whether Plaintiffs had standing to bring the case in the first place").

B. Plaid's Statutory Violations Establish Injury In Fact

Plaintiffs also have standing to bring their claims under the CFAA, CDAFA, SCA, and CAPA for the additional reason that those statutes afford them that right. Where the legislature codifies a statutory right that protects against "the risk of real harm," a plaintiff need not "allege any *additional* harm beyond the one identified by Congress." *Spokeo*, 136 S. Ct. at 1544. *See also Matera v. Google,* *Inc.*, No. 15-4062, 2016 WL 5339806, at **9, 14 (N.D. Cal. Sept. 23, 2016).

Congress and the California legislature granted citizens the means to enforce a right to privacy with respect to electronically stored information (CFAA, CDAFA, SCA), and solicitation of the same (CAPA). These statutes protect consumers, respectively, from unauthorized access to computers housing private information, at the federal level (*see* ¶¶ 270-98)[8] and in California (¶¶ 364-78);[9] from unauthorized access to stored information itself (¶¶ 299-312);[10] and from using deceit to solicit personal information from another person online (¶¶ 349-55).[11] Plaid's unauthorized solicitation, access, collection, and distribution of Plaintiffs' electronically stored private financial information "present the precise harm and infringe the same privacy interests" the legislatures sought to protect. *Van Patten*, 847 F.3d at 1043. These statutes' protections are an extension of traditional common law and Constitutional principles, applied by the legislature to the context of electronically stored and transmitted information. *See Facebook Internet Tracking*, 956 F.3d at 599 ("Advances in technology can increase the potential for unreasonable intrusions into personal privacy") (citation omitted). Thus, Plaid's violation of these statutes gives rise to a concrete injury sufficient to confer standing. *See Spokeo*, 136 S. Ct. at 1548.

[8] In addition to "computer crime" such as "trespass," Congress passed the CFAA to address "privacy protections." S. Rep. 99-432 at 2484 (1986); Congress reaffirmed this purpose by amending the CFAA in 1996 to fill in "gaps" in "privacy protection coverage." S. Rep. 104-357, at *4 (1996). *See also* Vasileios Karagiannopoulos, *From Morris to Nosal: The History of Exceeding Authorization and the Need for a Change*, 30 J. Marshall J. Info. Tech. & Privacy L. 465, 467 (2014) ("[A]mendments to the CFAA have expanded its scope in parallel with the increasing importance of computer systems and information contained in them to protect the privacy of information"). For example, 1030(a)(2) was amended specifically to "increase ***protection for the privacy*** and confidentiality of computer information" S. Rep. 104-357, at *7 (1996) (emphasis added).

[9] *See* Cal. Pen. Code § 502(a) (legislative intent is to "expand the degree of protection afforded to individuals . . . protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the ***protection of the privacy*** of individuals")(emphasis added).

[10] The SCA "codif[ies] a substantive right to privacy." *Facebook Internet Tracking*, 956 F.3d at 598 (citing *Campbell*, 951 F.3d at 1117-19); *id.* (citing S. Rep. No. 99-541, at 3 (1986) (the SCA was "modeled after the Right to Financial Privacy Act, 12 U.S.C. §§ 3401 *et seq.* to protect privacy interests in personal and proprietary information . . . .")). *See also Google Referrer Header Privacy*, 2020 WL 3035796, at *7 (SCA "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage") (citation omitted).

[11] CAPA's history shows that lawmakers were concerned with protecting consumers from requests for personal information by entities impersonating other businesses whose reputations and customer relationships would provide comfort to consumers in providing such data. *See infra* Arg. § VI-E).

C. Plaintiffs Have Standing To Seek Disgorgement Of Plaid's Unjustly-Earned Profits

Plaintiffs also have standing to recover the equitable relief they seek[12] due to Plaid's gains achieved through its violations of their dignitary rights, invasions of their privacy, and illicit use of their private information. "California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss." *Facebook Internet Tracking*, 956 F.3d at 599-600 (citations omitted).

The Ninth Circuit has explained that "an entitlement to unjustly earned profits" sufficient to confer Article III standing for California state law claims is established where plaintiffs allege that "they retain a stake in the profits garnered from their personal [data] because 'the circumstances are such that, as between the two [parties], it is *unjust* for [defendant] to retain it.'" *Id.* at 600 (holding that Article III was satisfied on this basis as to claims for, *inter alia*, common law fraud and violations of the CDAFA) (citation omitted). In *In re Facebook*, that was established through allegations that Facebook profited by selling the plaintiffs' internet browsing history data.

Here, Plaintiffs allege that Plaid has built a very successful business, generating tens of millions of dollars annually, by deceiving Plaintiffs to collect, use, and sell their data to companies such as the Apps. *Supra* Facts §§ A-C. These allegations are "sufficient at the pleading stage to demonstrate that [Plaid's] profits were unjustly earned." *Facebook Internet Tracking*, 956 F.3d at 601. *See also Google Referrer Header Privacy*, 2020 WL 3035796, at *10 (allegations that Google profited from disclosing plaintiffs' search terms to its advertisers without their consent and despite promises to the contrary "'sufficiently alleged a state law interest whose violation constitutes an injury sufficient to establish standing'" (quoting *Facebook Internet Tracking*, 956 F.3d at 601).

D. Plaintiffs' Economic Injury Is Well-Pled

Plaintiffs' allegations of economic injury—specifically, loss of indemnification rights; loss of regulatory protections over personal financial data; loss of control over personal data; increased risk of identity theft and fraud, and corresponding need to expend time and resources—although not required,

[12] *See* ¶ 268 (Intrusion); ¶ 325 (unjust enrichment); ¶ 347 (Cal. Constitution); ¶ 355 (CAPA); ¶ 363 (Deceit); ¶ 378 (CDAFA). Plaintiffs, as the owners of the data at issue, also have standing to seek, *inter alia*, disgorgement of that data by Plaid under the UCL. ¶ 336.

provide independent additional grounds to support standing. Plaid's arguments in response fail.

First, Plaid argues that Plaintiffs' claims of economic injury are conjectural. However, under Ninth Circuit law, a risk of future identity theft can constitute an injury in fact. *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010). Plaid's citation to *Katz v. Pershing LLC*, 672 F.3d 64, 70 (1st Cir. 2012), which is non-governing law that has been expressly contrasted to Ninth Circuit law,[13] is misplaced. Plaintiffs are not required to wait until the harms materialize before filing suit. *See also In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1054 (N.D. Cal. 2012) (injury properly alleged based on "increased, unexpected, and unreasonable risk to the security of [plaintiffs'] sensitive personal information," where plaintiffs alleged that defendant communicated their data to third parties without consent). Plaid is a particularly attractive target for a data breach: it has the banking information of **one in four people with a U.S. bank account**, (¶ 57), and the ABA has acknowledged the outsized security risks that Plaid faces. ¶ 79(f) (noting that "the sheer volume and value of the aggregated data make data aggregators a priority target for criminals, including identity thieves"). Plaid's cases are inapposite because they involved significantly less sensitive data, such as names, drivers' licenses, and anonymous social media browsing history—nothing like the consolidated banking data and access credentials of millions of financial accounts—and the circumstances were otherwise different. MTD at 11. Plaintiffs' mitigation measures are justified. As to indemnification, Plaintiffs' allegation is not that they "*could*" lose indemnification rights, as Plaid suggests (*id.*); it is that they *have* lost them, and they are presently-possessed personal property rights. *See Singer Co. v. Superior Court*, 179 Cal. App. 3d 875, 890 (1986) (describing the loss of partial indemnity as a deprivation of a "property right"); *see also Beltran v. United States*, 441 F.2d 954, 960-61 (7th Cir. 1971) (recognizing the loss of a right to indemnification as a loss of personal property).

Second, Plaid claims Plaintiffs do not specifically identify which regulatory protections they lost due to Plaid's conduct. MTD at 10. Yet Plaintiffs' allegation—that Plaid's removal of their data from the secure banking environment stripped it of regulatory safeguards—is supported by a February 2017 response from the ABA to an RFI from the CFPB recognizing the loss of these protections, and thus is

[13] *See Wilding v. DNC Servs.*, No. 16-61511, 2017 WL 6345492, at *7 (S.D. Fla. Aug. 25, 2017), *aff'd*, 941 F.3d 1116 (11th Cir. 2019) (contrasting *Krottner* and *Katz*).

more than sufficient at this stage to "plausibly" allege injury based on this loss. ¶¶ 215-24. *See Zappos.com*, 888 F.3d at 1022 ("[C]ontentions about the absence of certain facts . . . may be appropriate for summary judgment" but not "at the motion to dismiss stage.").

Third, although Plaid suggests otherwise, courts nationwide have recognized that loss of control over one's personally identifying information constitutes a cognizable harm sufficient to confer standing. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020) ("[T]he growing trend across courts that have considered this issue is to recognize the lost property value of [PII]." (citing cases)); *accord State v. Mayze*, 622 S.E.2d 836, 841 (Ga. 2005) ("identity fraud is an offense against the victim's possessory interest in his or her personal information"). As the Ninth Circuit has held, the loss of value of such information gives rise to damages, irrespective of whether the plaintiffs participated in the market for personal information. *In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014); *see also Svenson v. Google Inc.*, No. 13-04080, 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016) (mobile app user plaintiff alleged injury-in-fact based on diminution of value of PII disseminated by Google to third parties). The lone case cited by Plaid, *In re Google, Inc. Privacy Policy Litig.*, pre-dated *Facebook Privacy*, and does not alter the analysis here. No. 12-01382, 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013). The allegations are sufficient: Plaid's merits-based challenges to Plaintiffs' injury-in-fact must await a full record.

E. <u>Plaintiffs' Injuries Are "Fairly Traceable" To Plaid's Conduct, And Redressable</u>

Plaid's argument that Plaintiffs' injuries are not "fairly traceable" to its misconduct because Plaintiffs do not allege linking a bank account through Plaid is erroneous, as discussed *supra*, Facts § II. Plaintiffs' allegations suffice to establish a causal nexus between Plaid's conduct and their injuries.

With respect to redressability, courts have consistently recognized that violation of privacy rights can be redressed by an award of damages, *i.e.*, such remedy provides more than "psychic satisfaction," MTD at 14-15[14] *See Facebook Consumer Privacy*, 402 F. Supp. 3d at 784 ("[T]he Ninth Circuit has

[14] In the case cited by Plaid, *Steel Co. v. Citizens for a Better Environment*, the Supreme Court held that because the civil penalties authorized by the statute at issue were payable to the United State Treasury, the plaintiff-respondent "seeks not remediation of its own injury . . . but vindication of the rule of law . . ." 523 U.S. at 106. There is no comparable concern at issue here, where the statutory damages would be paid to Plaintiffs for remediation of their injury.

repeatedly explained that intangible privacy injuries can be redressed in the federal courts.”). The injunctive relief sought by Plaintiffs—*inter alia*, deleting existing data and terminating Plaid’s practice of harvesting and profiting from user’s personal financial data—would redress future harms suffered by Plaintiffs. *See Jewel v. Nat’l Sec. Agency*, 673 F.3d 902, 912 (9th Cir. 2011) (ruling that there was “no real question about redressability” when a plaintiff sought “an injunction and damages, either of which is an available remedy”). Plaintiffs thus “easily meet[] the third prong of the standing requirement.” *Id.*[15]

IV. Plaintiffs’ Claims Are Timely

Plaid does not challenge the allegations that are plainly within the statutes of limitations, including as to the multiple Plaintiffs whose data Plaid first took within the last couple of years, or the fact that Plaid continues to pull data to this day from Plaintiffs regardless of when the misconduct began. Each discrete breach by Plaid of its continuing obligations “may be treated as an independently actionable wrong with its own time limit for recovery.” *Aryeh v. Canon Bus. Sols., Inc.*, 55 Cal. 4th 1185, 1199 (2013). Each time Plaid updates its cache of Plaintiffs’ data, and/or monetizes the data, it commits a discrete, independently actionable wrong. ¶¶ 59-65

To the extent Plaid challenges the timeliness of some claims—its argument is vague—based on the fact that certain Plaintiffs first had their data taken by Plaid as far back as 2014 (*e.g.*, ¶ 150), this argument fails. Plaintiffs’ claims are subject to the “discovery rule,” *i.e.*, the rule that accrual of a cause of action is postponed “until the plaintiff discovers, or has reason to discover, the cause of action.” *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 807 (2005); *Mangum v. Action Collection Serv., Inc.*, 575 F.3d 935, 940 (9th Cir. 2009); 18 U.S.C. § 1030(g) (CFAA discovery rule); 18 U.S.C. § 2707(f) (SCA discovery rule). “A plaintiff has reason to discover a cause of action when he or she has reason at least to suspect a factual basis for its elements.” *Fox*, 35 Cal. 4th at 807 (citation omitted). “Resolution of the statute of limitations issue is normally a question of fact.” *Id.* at 810.

Plaintiffs allege that when they linked their bank accounts they were unaware of the existence or

[15] Finally, Plaid does not dispute Plaintiffs’ standing to pursue injunctive relief. This requires showing “either continuing, present adverse effects’ due to their exposure to [Plaid’s] past illegal conduct or a sufficient likelihood that they will again be wronged in a similar way.” *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1120 (9th Cir. 2020) (internal quotation marks and alterations omitted). Plaintiffs allege Plaid’s ongoing retention, use, and sharing of the data it collects.

role of Plaid; unaware of providing login credentials to Plaid; and unaware that Plaid would collect, receive, store, use, and sell their banking information. ¶¶ 100-207. Plaintiffs' allegations make clear that they did not uncover Plaid's misconduct until recently. ¶ 241. Plaintiffs further allege that they "could not have learned through the exercise of reasonable diligence of Plaid's conduct," ¶ 243, and the covert and deceptive nature of Plaid's operations lends ample support to this assertion. ¶¶ 26-77. Accordingly, Plaintiffs have adequately alleged that the applicable statutes of limitations did not begin to accrue until recently—certainly less than two years prior to filing—and that their claims are therefore timely.

In addition, or in the alternative, Plaid's fraudulent concealment tolls the statutes of limitations given that Plaid hid its misconduct, and Plaid is estopped from asserting them. *See Hexcel Corp. v. Ineos Polymers, Inc.*, 681 F.3d 1055, 1060 (9th Cir. 2012) ("A statute of limitations may be tolled if the defendant fraudulently concealed the existence of a cause of action in such a way that the plaintiff, acting as a reasonable person, did not know of its existence."); *Britton v. Girardi*, 235 Cal. App. 4th 721, 734 (2015) (estoppel applies). Plaintiffs allege in detail Plaid's misleading statements and intentional concealment that continued up to and beyond the time the initial complaint was filed. While Plaid denies on the merits that it concealed the true facts of its conduct, this factual defense is premature.

V. <u>Plaintiffs' Equitable Claims Are Not Barred By Remedies at Law</u>

Plaid asserts that Plaintiffs' claims for unjust enrichment and under the UCL, and requested equitable remedies under all claims, are barred by the existence of an adequate remedy at law. MTD at 17. This is premature and ignores the remedies to which Plaintiffs are entitled under the applicable statutes (and that serve a distinct purpose that damages will not redress).

First, remedies at law alone would not make Plaintiffs whole. Plaintiffs seek to compel Plaid to take prospective action to protect consumers from future privacy invasions, including to "cease its misconduct, purge the data it has unlawfully collected, notify consumers of its misconduct, and inform consumers of the steps they can take to protect themselves from further invasions." ¶ 7. These are paradigmatic examples of prospective relief to address an ongoing harm, which money damages cannot adequately address. *See, e.g., LSH CO v. Transamerica Life Ins. Co.*, No. 18-09711, 2019 WL 3064422, at *15 (C.D. Cal. Mar. 20, 2019) ("Even if the monetary compensation that may be found . . . would properly compensate the alleged [unlawful conduct], Plaintiffs properly allege facts to show the necessity of an injunction to counter the threat of continuing misconduct.”).**[16]**

Second, Plaintiffs seek declaratory relief that would clarify and define the scope of Plaintiffs’ and Class members’ rights under the relevant statutory and common law, including Plaid’s obligations to transparently disclose to consumers the scope and nature of its practices. *E.g.*, ¶¶ 310, Prayer for Relief C. Federal Rule 57 provides that “[t]he existence of another adequate remedy does not preclude a declaratory judgment that is otherwise appropriate.” Fed. R. Civ. P. 57; *see also id.*, 1937 Advisory Committee Notes (“[T]he fact that another remedy would be equally effective affords no ground for declining declaratory relief.”). Ultimately, the “critical question is whether the declaratory relief ‘will serve a useful purpose in clarifying and settling the legal relations in issue.’” *T. K. v. Adobe Sys. Inc.*, No. 17-04595, 2018 WL 1812200, at *12–13 (N.D. Cal. Apr. 17, 2018) (citation omitted). Plaid possesses and profits from personal financial data from over 200 million unique accounts, and it continues to add data from those *and* new, unsuspecting users each day. Defining Plaid’s prospective legal obligations cannot be achieved through monetary damages.

Third, none of Plaid’s authority permits, let alone requires, a District Court to override clear direction from Congress in providing a statutory right to equitable relief under the CFAA and SCA. *See Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 842 (9th Cir. 2020).

Fourth, Plaid offers nothing to support its assertion that any of the legal remedies Plaintiffs seek are “plain, adequate, and complete.” Plaintiffs seek equitable disgorgement and restitution precisely because they are well-supported by the facts of this action, and damages tethered to individual losses may be incomplete. *See id.* at 844 n.8; *Am. Life Ins. Co. v. Stewart*, 300 U.S. 203, 214 (1937) (“A remedy at law does not exclude one in equity unless it is equally prompt and certain and in other ways efficient.”). In this case, the fact question of whether other remedies are complete and equally efficient for the Class will turn on the resolution of questions regarding Plaid’s profits, revenues, competitive advantage, and other valuable benefits derived from Plaintiffs’ and Class members’ data, and concerning the extent and manifestations of the harm Plaid has caused. Plaid’s authority confirms that its argument is premature. *Cf. Sonner*, 971 F.3d at 837-38 (affirming dismissal of CLRA claim for equitable

[16] Contrary to Plaid’s suggestion (MTD at 17), the law does not require recitation of the words “damages are inadequate.” Plaintiffs plead *facts* showing no adequate remedy at law exists, which is sufficient.

restitution "[o]n the brink of trial after more than four years of litigation," and after plaintiff defeated summary judgment on the alternative legal claim).[17]

Plaid's reference to court opinions that have dismissed claims for equitable relief at the pleading stage are distinguishable, and are against the weight of authority. While "[a] few federal courts seem to have decided that claims for equitable relief should be dismissed at the pleading stage if the plaintiff manages to state a claim for relief that carries a remedy at law,"[18] most courts have concluded that there is "no basis in California or federal law for prohibiting the plaintiffs from pursuing their equitable claims in the alternative to legal remedies at the pleadings stage." *Adkins v. Comcast Corp.*, No. 16-05969, 2017 WL 3491973, at *3 (N.D. Cal. Aug. 1, 2017). In fact, the Ninth Circuit has held that allowing a plaintiff to plead an equitable remedy that is "duplicative of or superfluous to" a plaintiff's other claims is *supported* by the Federal Rules, and does not warrant dismissal. *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762–63 (9th Cir. 2015). Similarly, courts in this district have concluded that "those decisions allowing claims for equitable relief to proceed as an alternative remedy, at the pleading stage" better reflect "the broad remedial purposes of the California consumer protection statutes." *Luong v. Subaru of Am., Inc.*, No. 17-03160, 2018 WL 2047646, at *7 n.6 (N.D. Cal. May 2, 2018) (denying dismissal of plaintiff's UCL claim, notwithstanding adequacy of remedies at law). Otherwise stated, "alternative remedial requests should be dealt with at the end of a case, not the beginning." *Wildin v. FCA US LLC*, No. 17-02594, 2018 WL 3032986, at *7 n.4 (S.D. Cal. June 19, 2018). Ultimately, Plaintiffs "may be required to make an election of remedies if [they] prevail[] on multiple claims." *Thompson v. Transamerica Life Ins. Co.*, No. 18-05422, 2018 WL 6790561, at *13 (C.D. Cal. Dec. 26, 2018). But this is not the time for such an election.[19]

[17] Indeed, *Sonner*—cited multiple times by Plaid—is uniquely inapposite to the facts of this case. "[L]ess than two months before trial," the plaintiff "voluntarily dismissed her sole state law damages claim and chose to proceed with only state law equitable claims for restitution and injunctive relief." 971 F.3d at 837-38. The Ninth Circuit was particularly troubled by the plaintiff's attempt "to try the class action as a bench trial rather than to a jury" so close to the trial date. *Id.* at 837. Further, plaintiff sought "the same sum in equitable restitution" as "she requested in damages to compensate her for the same past harm." *Id.* at 844. None of that holds true here.

[18] In *Philips v. Ford Motor Co.*, injunctive relief claims were dismissed where the plaintiffs **did not contest** that adequate legal remedies were available. No. 14-02989, 2015 WL 4111448, at *16 (N.D. Cal. July 7, 2015) (plaintiffs did "not even address the issue"), *aff'd*, 726 F. App'x 608 (9th Cir. 2018).

[19] While Plaintiffs concede Count 4 should be dismissed as a standalone cause of action, there is no basis to dismiss Plaintiffs' requests for declaratory and injunctive relief, predicated on other causes of

VI. Plaid's Rule 12(b)(6) Arguments Have No Merit

A. Plaintiffs Properly Plead Claims Under The California Constitution And For Common Law Invasion Of Privacy-Intrusion Into Private Affairs

Plaintiffs adequately allege that Plaid's conduct (*supra*, Facts § I-II) violated Plaintiffs' reasonable expectations of privacy in a highly offensive manner, stating claims for invasion of privacy under the California Constitution and under the California common law. Because the tests for these two claims are similar, "courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Facebook Internet Tracking*, 956 F.3d at 601 (citing *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)). Both issues present "mixed questions of law and fact." *Opperman*, 87 F. Supp. 3d at 1059 (citing *Hill v. NCAA*, 7 Cal. 4th 1, 40 (1994)). Thus, these claims may only be disposed as a matter of law if the *undisputed material facts* show no reasonable expectation of privacy or an insubstantial impact on privacy interests. *See id.* Plaid has failed to make that showing.

Plaintiffs plead a reasonable expectation of privacy. The types of information Plaid collected—login credentials, account numbers, and detailed financial records—are clearly those in which consumers have a reasonable expectation of privacy. *See United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (noting that financial records are reasonably "expected to be kept private"). The reasonableness of this expectation is reflected in longstanding custom and practice, security measures intended to prevent unauthorized access to banking account information, laws protecting a right to financial privacy, and assurances of protection by applications that use Plaid. *See* ¶ 272. In this case, it is not only the data itself that gives rise to these expectations, but also the amount of data at issue, a volume sufficiently comprehensive that it allows Plaid to generate detailed profiles of consumers' lives, habits, associations, and activities. ¶¶ 50, 64, 266-268, 345; *Cal. Bankers Ass'n v. Shultz*, 416 U.S. 21, 89-90 (1974) (Douglas, J., dissenting) ("One's bank accounts are within the 'expectations of privacy' category. For they mirror not only one's finances but his interests, his debts, his way of life, his family, and his civic commitments, . . . [They] may well record a citizen's activities, opinion, and beliefs as fully as transcripts of his telephone conversations."); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th

action. *See* ¶¶ 297, 310, 336-37, 355, 378; Prayer for Relief C, D.

Cir. 2019) (where “vast quantities of personal information” are involved, “[t]echnological advances provide ‘access to a category of information otherwise unknowable,’ and ‘implicate privacy concerns’” in new and different ways) (quoting *Riley v. California*, 573 U.S. 373, 393 (2014)). Plaid’s acts violated reasonable and well-established expectations shared across society.

Plaid asserts that Plaintiffs (and presumably the millions of class members) are somehow unlike typical consumers for whom these expectations are reasonable. This assertion is based entirely on Plaid’s disregarding the Plaintiffs’ allegations, and on the same legally and factually flawed consent arguments it raises throughout its motion. Plaid’s merits defenses do not establish that Plaintiffs’ privacy expectations were unreasonable as a matter of law.

Plaid’s intrusions were highly offensive. Plaintiffs also satisfy the second prong for pleading these privacy claims. “Determining whether a defendant’s actions were ‘highly offensive to a reasonable person’ requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder’s motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.” *Facebook Internet Tracking*, 956 F.3d at 606 (citation omitted). This requires a fact-intensive inquiry that “examines all of the surrounding circumstances.” *Hernandez*, 47 Cal. 4th at 295. Such an inquiry cannot be conducted at the motion to dismiss stage where, as here, there are open factual questions regarding “the degree and setting of the intrusion, the intruder’s motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.” *Facebook Internet Tracking*, 956 F.3d at 606. Those questions are best left for a trier of fact, with a full record.

Plaintiffs more than adequately plead that Plaid’s conduct was highly offensive (or, at a minimum, the offensiveness presents a question for the finder of fact). The Apps provide money transfer services, enabling users to send and receive money from their financial accounts. ¶ 31. By inserting itself into the account linking process, Plaid secretly accessed, stored, and sold data about every financial transaction Plaintiffs made, over a period of years, through any account that could be accessed using the credentials Plaid obtained. *Supra*, Facts § I-III. Even if Plaintiffs had known Plaid was *present* (which they did not), Plaid’s extraordinary intrusions—far exceeding anything reasonably related to verifying an account or sending and receiving funds—would still be unexpected, excessive, and offensive. Its intrusions also violate industry norms. ¶¶ 78-97. In circumstances less plainly egregious than this, courts have consistently held that collection of intimate or sensitive personally identifiable information may amount to a highly offensive intrusion. *See, e.g.*, *In re Vizio*, 238 F. Supp. 3d at 1233.

Plaintiffs' allegations concerning *how* Plaid obtained their data, *i.e.*, by representing itself to be trusted financial institutions and hiding its involvement as a third-party, further underscores the offensive and misleading nature of Plaid's practices. "[D]eceit can be a 'kind of "plus" factor [that is] significant in establishing an expectation of privacy or making a privacy intrusion especially offensive.'" *Heeger v. Facebook, Inc.*, No. 18-06399, 2019 WL 7282477, at *4 (N.D. Cal. Dec. 27, 2019) (quotation omitted); *see also In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 150-51 (3d Cir. 2015) ("What is notable about this case is how Google accomplished its tracking . . . . Characterized by deceit and disregard, the alleged conduct raises different issues than tracking or disclosure alone.") (applying California law).

None of Plaid's authorities hold or even imply that the conduct alleged here is inoffensive—it plainly is not. Plaid's cited cases involve defendants that compiled far less sensitive information, in both scope and content, than here. *See Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) (defendant engaged in "routine commercial behavior" by requesting zip codes to procure home address to mail marketing materials); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (anonymized LinkedIn ID and URL data, disclosing browsing history among LinkedIn profiles); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1050 (N.D. Cal. 2012) (collection of sporadic location data and basic personal information by developers from mobile devices). Those cases simply cannot be compared to the multi-year, expansive, deeply personal privacy invasions involving sensitive data alleged here. *See also Opperman*, 205 F. Supp. 3d at 1078-79 (distinguishing *Folgelstrom* because it did not involve the surreptitious theft or any data "more private than a person's mailing address," and criticizing *In re iPhone* for failing to "explain how expansion of *Folgelstrom*'s holding, counter to the privacy interests of iDevice users, was consistent with California's privacy norms."). *See also* ¶¶ 262-65, 342-46. Accordingly, the Court should reject Plaid's argument that its actions were not, as a matter of law, sufficiently serious. *See Facebook Internet Tracking*, 956 F.3d at 606 (concluding that "Plaintiffs' allegations of surreptitious data collection when individuals were not using Facebook are sufficient to survive a dismissal motion" on whether Facebook's "[data] collection practices could highly offend a reasonable individual").

B. Plaintiffs Have Properly Pleaded Claims Under The UCL

Plaid raises several arguments against Plaintiffs' UCL claims, but none have merit.

Plaintiffs lost money or property. Under the UCL's "lost money or property" requirement, a plaintiff must show "'some form of economic injury'" such as "'having a present or future property interest diminished.'" *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1093 (N.D. Cal. 2018) (quoting *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 323 (2011)). "'At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice.'" *Id.* (quoting *Kwikset*, 51 Cal. 4th at 327).

Unlike the cases cited by Plaid, Plaintiffs have not alleged the loss of information such as their names and addresses (*see Archer v. United Rentals, Inc.*, 195 Cal. App. 4th 807, 813, 816 (2011)) or the content of Facebook messages (*see Campbell v. Facebook*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014). As discussed *supra*, Facts § III, Plaintiffs have suffered economic injuries (*i.e.*, lost money or property), including in the form of lost indemnity rights that existed when Plaintiffs' data was held at their banks. Those economic injuries are sufficient to survive a pleadings challenge. *See Gonzales*, 305 F. Supp. 3d at 1093 (allegations that Uber intercepted private communications satisfied the lost money or property requirement when combined with allegations that the communications were used to reduce the supply of drivers, thereby increasing wait times and ultimately decreasing drivers' earnings).

In addition, Plaintiffs have alleged that they would not have connected their bank accounts to the Apps the way they did (for the purpose of transferring money) if they had known the truth about Plaid's role and its practices. *See, e.g.*, ¶¶ 105, 116. Those allegations also establish standing under the UCL. *See Romero v. Securus Techs., Inc.*, 216 F. Supp. 3d 1078, 1091 (S.D. Cal. 2016) (allegations that the plaintiffs "would not have paid for and used" a telephone system had they known the calls were being recorded was sufficient for lost money or property element).

Plaid's "unlawful" business practices: Plaid's conduct is "unlawful" under the UCL because it violated the following statutes and regulations: (1) CFAA; (2) SCA; (3) CDAFA; (4) CAPA; (5) Cal. Civ. Code § 1709; (6) Article 1, § 1 of the California Constitution; (7) CalFIPA, Cal. Fin. Code § 4051, *et seq.* ; (8) CalOPPA, Cal. Bus. & Prof. Code § 22575, *et seq.*; and (9) the GLBA's Privacy Rule, 16 C.F.R. § 313, and Reg. P, 12 C.F.R. Part 1016. ¶ 330. As to the first five violations, Plaid relies upon its arguments against Plaintiffs' claims based upon the same provisions. MTD at 20. Plaid's challenges to those claims as a UCL predicate fail for the reasons discussed elsewhere in this brief. Plaid fails to address the California constitutional predicate, which is valid. *See Goodman v. HTC Am., Inc.*, No. 11-1793, 2012 WL 2412070, at *12 (W.D. Wash. June 26, 2012).

As for the violations of the GLBA's Privacy Rule and CalFIPA, Plaid argues that those statutes "preclude a private right of action," and thus cannot support a UCL claim. MTD at 20. As a general matter, "'[v]irtually any state, federal or local law can serve as the predicate for an action under section 17200,'" *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 841 (quoting *Davis v. HSBC Bank Nevada*, 691 F.3d 1152, 1168 (9th Cir. 2012)). A private right of action is no prerequisite. *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 182-83 (1999); *Kasky v. Nike, Inc.*, 27 Cal. 4th 939, 950 (2002) (UCL action permitted "even when 'the conduct . . . violates a statute for the direct enforcement of which there is no private right of action'") (citation and quotation marks omitted). Rather, "[t]o forestall an action under the [UCL], another provision must actually 'bar' the action or clearly permit the conduct." *Cel-Tech*, 20 Cal. 4th at 183. Neither the GLBA nor CalFIPA explicitly bars a private UCL claim. In fact, a court from this District approved an "unlawful" UCL claim based upon the violation of the GLBA. *See In re Anthem Data Breach Litig.*, 162 F. Supp. 3d 953, 989 (N.D. Cal. 2016). Plaid's argument that it did not violate certain provisions in the GLBA and CalFIPA in light of partial exemptions for requests authorized by consumers (MTD at 20 n.16) begs the question by assuming that Plaintiffs authorized or requested Plaid to collect, transfer, and sell their private banking information. They did not. *Supra,* Facts § I and Arg. § II.

Plaid argues that CalOPPA cannot serve as the basis for Plaintiffs' "unlawful" UCL claim because they do not allege they purchased or leased anything from Plaid. MTD at 20-21. CalOPPA defines "consumer" as "any individual who ***seeks*** or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes." Cal. Bus. & Prof. Code § 22577 (emphasis added). Plaintiffs sought services for personal purposes: the use of "seek" indicates that the statute does not require money to have changed hands. Plaid also drops a footnote to argue that it did not violate CalOPPA for a handful of reasons. MTD at 21 n.17. Because Plaid operated both consumer-facing web-based software and a behind-the-scenes online software (¶¶ 31-32), Plaid clearly constitutes an "operator," and its arguments based upon "online service" status under CalOPPA are unavailing.

Plaid's "unfair" business practices: Plaid's conduct is "unfair" under the UCL because it violated California's public policy of protecting consumers' privacy interests by surreptitiously collecting Plaintiffs' bank login information, using that information to access their bank accounts, accessing and copying private banking data, selling that data to the Apps, and storing and using that data for its own purposes, all without consent. ¶ 331. Plaid violated important public interests protected by the laws under which Plaintiffs' claims are brought. ¶ 332. Plaid's conduct did not create a benefit outweighing these strong public policy interests, but instead benefitted Plaid at the expense of consumers' privacy. ¶ 333.

If the detailed facts alleged in the CAC could be deemed conclusory, as Plaid asserts (MTD at 21), it is difficult to imagine the complaint that could pass muster under Rule 8. Stealing the private login credentials of millions of consumers obviously offends public policy, is immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers. *See McDonald v. Coldwell Banker*, 543 F.3d 498, 506 (9th Cir. 2008). Surreptitiously accessing hundreds of millions of bank accounts is unfair. Stealing years of private banking data is unfair. Profiting off that data without permission is unfair. Plaintiffs need plead nothing more under any test. *See In re Webkinz Antitrust Litig.*, 695 F. Supp. 2d 987, 998-99 (N.D. Cal. 2010) ("the central issue presented under [the UCL] is whether the public at large, or consumers generally, are affected by the alleged unlawful business practice").

Plaid's "fraudulent" business practices: Plaid engages in "fraudulent" business practices by (1) mimicking bank websites in its software to surreptitiously collect consumers' private bank login information; (2) using consumers' private bank login information to access their bank accounts and use their data as alleged, all without consent. ¶ 334. Plaid's business practices are both likely to deceive members of the public and already have accomplished widespread public deception. *Id.*

Plaid raises a single challenge to this claim, arguing that Plaintiffs fail to satisfy Rules 8 and 9(b). MTD at 21-22. As discussed *infra* at Arg. § VI-F, however, Plaintiffs' fraud-based allegations more than satisfy the Rule 9(b) standard. And Plaintiffs show their reliance upon Plaid's uniform omissions and misleading partial representations by alleging that they would not have connected their bank accounts to the Apps the way they did if they had known the truth about Plaid and its practices. *See, e.g.*, ¶¶ 4, 35-41, 47, 105, 116, 334, 360-61. Those uniform omissions are material and thus support a presumption of reliance. *See Daniel v. Ford Motor Co.*, 806 F.3d 1217, 1225 (9th Cir. 2015) (citing *In re Tobacco II Cases*, 46 Cal. 4th 298, 327 (2009)).

Plaintiffs' entitlement to restitution and disgorgement: The UCL provides that "[t]he court may make such orders or judgments . . . as may be necessary to restore to any person in interest any money or property, real or personal, which may have been acquired by means of such unfair competition." Cal. Bus. & Prof. Code § 17203. Here, Plaintiffs seek (1) restitution, (2) "disgorgement by Plaid of the wrongfully-obtained private data obtained from their financial accounts, including without limitation a return of that data to Plaintiffs and Class members and the Plaintiffs' and Class members' financial institutions with corresponding protections and security," and injunctive relief. ¶ 336.

While Plaintiffs are in fact entitled to restitution for the economic value that Plaid derived from unlawfully accessing their banking accounts and data—an especially important remedy when there are severe violations of privacy and dignitary interests—they are not, contrary to Plaid's argument (MTD at 22), seeking such remedy *under the UCL*. Under the UCL, Plaintiffs seek only disgorgement of their property in the form of the data Plaintiffs unwittingly allowed Plaid to take from them. Plaid established the market for the personal data extracted from Plaintiffs' banks by arranging to siphon it out and sell it to the Apps, in addition to using the data to sell value-added products. In the "but-for" world, Plaintiffs would not have connected the Apps to their banks through Plaid, but instead would have followed a standard microdeposit procedure that would have (1) left Plaid out of the picture completely, and (2) left Plaintiffs' private data secure in their banks. But as a result of Plaid's deception, Plaintiffs lost control over the data that Plaid took and sold behind their backs. Disgorgement of the data itself Plaid wrongfully took from their banks (or the value thereof) is properly sought under the UCL.

C. <u>Plaintiffs Have Properly Pleaded Claims Under The CFAA And CDAFA</u>

Plaid addresses its arguments against Plaintiffs' CFAA and CDAFA claims in tandem, and Plaintiffs reply in kind. MTD at 22-29. As discussed below, none of Plaid's arguments have any merit.

The CFAA and CDAFA apply to the facts as alleged. Plaid first argues that the CFAA and

CDAFA are “anti-hacking” statutes (MTD at 22), but neither statute is limited to a stereotypical hacking operation on the dark web. For example, the CFAA’s prohibition on accessing a computer “without authorization” may be violated “when a person circumvents a computer’s generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer.” *HiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1003 (9th Cir. 2019). That prohibition extends to where otherwise valid login credentials are used by a party who lacks authority to use them. *See United States v. Nosal,* 844 F.3d 1024, 1034 (9th Cir. 2016) (use of another party’s login credentials may violate the CFAA where permission to access has been revoked); *Calsoft Labs, Inc. v. Panchumarthi*, No. 19 -04398-NC, 2020 WL 512123, at *10-11 (N.D. Cal. Jan. 31, 2020) (use of “legitimate access credentials” may violate the CFAA where the party lacked permission to use them).[20]

As a result, Plaid’s argument that Plaintiffs do not allege “facts suggestive of hacking” (MTD at 23) is irrelevant, and ignores that Plaintiffs have in fact alleged that Plaid acted as an unauthorized, unknown bad actor when it obtained and used consumers’ bank login credentials, then collected, transferred, sold and used consumers’ private banking data without their permission. Those facts suffice.

Plaintiffs have standing under the CFAA and CDAFA. Plaid next argues that Plaintiffs lack standing because they have not pleaded “economic damages” under the CFAA and “damage or loss” under the CDAFA. *Id*. The CFAA permits any person who suffers damage or loss by reason of a violation to sue a violator whose conduct causes economic losses to “1 or more persons” of at least $5,000 during a one-year period. *See* 18 U.S.C. §§ 1030(g) & (c)(4)(A)(i)(I).[21] The CDAFA does not impose a minimum damages requirement, but instead provides a civil claim for one who suffers any “damage or loss by reason of a violation.” Cal. Pen. Code § 502(e)(1); *see also Facebook, Inc. v. Power Ventures, Inc.*, No. 08-05780, 2010 WL 3291750, at *4 (N.D. Cal. July 20, 2010).

Plaintiffs have pleaded the required economic losses (or damage and loss), including losses of at least $5,000 during a one-year period. Under the CFAA, damages may be aggregated across class members to meet the $5,000 minimum. *See In re Apple & AT&TM Antitrust Litig.*, 596 F. Supp. 2d

[20] *See also supra*, Arg. § III-B, n.9 & n.10 (discussing legislative intent).

[21] Plaid is incorrect in arguing that Plaintiffs’ claim for injunctive and other equitable relief must be dismissed. MTD at 23 n.19. The statute allows a civil plaintiff to recover “compensatory damages ***and injunctive or other equitable relief***.” 18 U.S.C. § 1030(g) (emphasis added).

1288, 1308 (N.D. Cal. 2008) ($5,000 threshold could be met by aggregating individual damages, such as diminution of value of the plaintiffs' iPhones). Multiple intrusions may combine over a one-year period to meet the $5,000 minimum. *See Creative Computing v. Getloaded.com, LLC*, 386 F.3d 930, 934-35 (9th Cir. 2004); *In re Toys R Us, Inc., Privacy Litig.*, No. 00-2746, 2001 WL 34517252, at *10 (N.D. Cal. Oct. 9, 2001) (allegations that defendant caused a file to be implanted in each of plaintiffs' computers at various points, causing damages including misappropriating the economic value of their "personality," showed aggregated damages exceeding $5,000 in one year).

When Plaid removed consumers' data from the secure banking environment, the lost value of their indemnification rights alone clearly exceeds $5,000, especially considering the Class includes tens of millions of consumers, many of whom must have had substantial funds in their accounts. *See* ¶¶ 54, 215-24. It is proper to aggregate Class losses to meet the minimum threshold, especially because (1) Plaid used the same methods to intrude upon Plaintiffs' and the Class members' financial accounts and the data in those accounts (¶ 49); and (2) Plaid deployed the same software templates in the Apps to intrude upon and compromise the integrity of Plaintiffs' and the Class members' mobile devices (¶ 39 n.22). *See Creative Computing*, 386 F.3d at 934-35; *Apple & AT&TM Antitrust*, 596 F. Supp. 2d at 1308.

Plaid also attempts to argue that Plaintiffs lack standing to sue under § 502(c)(3), (6) & (7) of the CDAFA because standing "only exists for the *owner* of the computer services or computer attacked and damaged." MTD at 23 (emphasis in original). But the CDAFA provides a private right of action for "the owner or lessee of the . . . ***data***" in addition to the owner of the computer itself. Cal. Pen. Code § 502(e)(1); *accord Gonzales*, 305 F. Supp. 3d at 1090. Plaintiffs own the private banking data at issue.

Plaid accessed a computer or data without authorization. Plaid asserts that Plaintiffs do not plausibly allege that it accessed any computer or data without authorization because "Plaintiffs chose to link their accounts (whether through Plaid or not)" and because "Plaid's Privacy Policy lists the data Plaid can collect." MTD at 26-27. Both arguments fail. As discussed *supra* at Arg. § II, Plaid's privacy policy-based argument is meritless and cannot be decided on a motion to dismiss. And, consumers routinely authorize money transfers to and from accounts, such as for automatic payments and deposits, with no expectation that their banking data is being disclosed. Nothing about that general proposition lends any support to the idea that Plaintiffs gave permission to Plaid, or for Plaid's conduct—an idea refuted throughout the CAC. Plaid comes nowhere close to demonstrating the unambiguous authorization that would be required to defeat Plaintiffs' claims on a motion to dismiss. *See, e.g., Apple & AT&TM Antitrust*, 596 F. Supp. 2d at 1308 (rejecting Apple's argument that plaintiffs' CFAA claims failed because they alleged that they authorized a software update, noting that plaintiffs did not authorize damage to their iPhones, Apple's warning in connection with the update was ambiguous, and some downloading of the update was "unsuspected").[22]

Plaintiffs plead facts showing "damage" under the CFAA and CDAFA. Plaid next argues that Plaintiffs fail to allege "damage" for a claim under CFAA §§ (a)(5)(A)-(C) because simply downloading data does not impair the integrity of the data or systems. MTD at 27. Contrary to Plaid's suggestion, "'courts in the Ninth Circuit have expressly held that, under the CFAA, "it is not necessary for data to be physically changed or erased to constitute damage to that data." *Satmodo, LLC v. Whenever Commcns., LLC*, No. 17-0192, 2017 WL 6327132, at *3 (S.D. Cal. Dec. 8, 2017) (quotations omitted); *see also Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 894-95 (N.D. Cal. July 20, 2010) ("[i]t is sufficient to show that there has been an ***impairment to the integrity of data***") (emphasis added; quoting 18 U.S.C. § 1030(e)(8)).

In *Shurgard Storage Centers, Inc., v. Safeguard Self Storage, Inc.*, the plaintiff alleged that an employee accessed its computer system and emailed proprietary information to the defendant, without otherwise damaging its computers. 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000). The court found the plaintiff had thereby adequately alleged "damage" under the CFAA because an "impairment to integrity" had occurred even though no data was physically changed or erased. *Id.* at 1126; *see also Therapeutic Research Faculty v. NBTY, Inc.*, 488 F. Supp. 2d 991, 996-97 (E.D. Cal. 2007) (finding that unauthorized access to a computer system and disclosure of its information may constitute an

[22] Plaid argues that Plaintiffs' lack of notice of its privacy policy "cannot form the basis for a claim" under the CFAA or CDAFA because there can be no violation if the defendant "reasonably could have thought" it had permission. MTD at 27 n.24. That argument conflates Plaid's state of mind with Plaintiffs' notice of and consent to be bound to the terms of Plaid's policy. It also ignores well-pled allegations that Plaid acted with the intent to deceive. *See, e.g.*, ¶ 74(d). *Cf. Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016) (citing summary judgment evidence that end users gave the defendant permission to share a promotion, and thus—arguably—permission to use Facebook's computers).

impairment to integrity even though no data was physically changed or erased).

Plaintiffs have adequately alleged impairment to the integrity of their data by alleging Plaid (1) deceptively acquired their bank login credentials and gained access to their banking data, thereby destroying their valuable indemnity rights; (2) took their data out of their banks' secure environment and sold it without adequate controls over what purchasers would do with it; (3) obtained an open connection to their accounts so that it could control access to, and steal information from, the banks' computer systems; (4) installed software in the Apps to capture their sensitive bank login data; and (5) accessed Plaintiffs' banks' computer systems, copied their banking data, sold it to the Apps, and used it for its own purposes. ¶¶ 214-27, 285(a)-(d), 288(a)-(d), 291(a)-(d).[23]

Moreover, courts also recognize "damage" under the CFAA where, as here, software is used to alter the controls of a computer and the integrity of the system is thereby impaired. *See Microsoft Corp. v. Mutairi*, No. 14-00987, 2015 U.S. Dist. LEXIS 95541, at *3 (D. Nev. June 25, 2015) (program caused "damage" to computers because it was able to "steal information from the computer, control the computer, and upload data to the computer"); *GM L.L.C. v. Autel.US Inc.*, No. 14-14864, 2016 WL 1223357, at *10 (E.D. Mich. Mar. 29, 2016) (finding impaired integrity of a computer system where the defendants copied information and shared usernames with unauthorized users, leading to unauthorized use of accounts and downloads); *Microsoft Corp. v. Doe*, No. 14-00811, 2015 WL 4937441, at *9 (E.D. Va. Aug. 17, 2015) (finding "damage" where software allowed defendants to take control of computers, then extract sensitive, personal information and funds from bank accounts).

Here, Plaid impaired the integrity of Plaintiffs' smartphones when it installed software in the Apps to capture their sensitive bank login data. ¶¶ 285(c), 288(c), 291(c). Plaid also impaired the integrity of their banks' computer systems, including when it (1) deceptively accessed those systems and destroyed Plaintiffs' valuable indemnity rights; and (2) obtained an open connection to steal information from those systems. ¶¶ 214-24, 285(b), 288(b), 291(b). *See United States v. Yücel*, 97 F. Supp. 3d 413, 419-20 (S.D.N.Y. 2015) (by causing a computer to "be operated by unauthorized users who have the

[23] In addition to incurring "damage," Plaintiffs also incurred "loss" under CFAA § 1030(e)(11) due to the loss of their valuable indemnification rights and additional data protections, as well as the loss of their data itself. ¶¶ 292, 297.

capability of extracting confidential information from the computer's hard drive," the defendant impaired the "uncorrupted condition" of the computer system because "the system no longer operates as it did" and "the economic value of the computer system" was "negatively impact[ed]").

The cases Plaid cites are distinguishable because Plaid did not "simply download[]" Plaintiffs' data "without leaving a trace." *Fidlar Techs. v. LPS Real Estate Data Sols., Inc.*, 810 F.3d 1075, 1084 (7th Cir. 2016). Rather, Plaid uses its software to compromise the security of Plaintiffs' banks' computers on an ongoing basis. *See NetApp v. Nimble Storage, Inc.*, No. 13-05058, 2015 WL 400251, at *14 (N.D. Cal. Jan. 29, 2015) ("[C]opying *information* does not necessarily render computer systems less secure, because copying information on its own does not necessarily allow a hacker to access other systems, programs, or data.") (emphasis in original); *Yücel*, 97 F. Supp. 3d at 421 (distinguishing cases finding no damage where data was copied because the defendants did not "install a program on the target computer that compromised the computer's security on an ongoing basis").[24]

Plaid also argues that Plaintiffs' claims under Sections 502(c)(1) and (c)(4) of the CDAFA fail because damage to the integrity of computers and data is not recognized as "damage" under that statute. MTD at 27-28. In the single case Plaid cites in support of its argument, *Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147 (C.D. Cal. 2018), there was no allegation of damage to the integrity of a computer or data similar to the types of "damage" routinely recognized for claims under the CFAA. The court found that it was not enough to show damage or use under Sections 502(c)(1) and (c)(4) of the CDAFA where the plaintiff alleged that the defendants used bots to access its public-facing website and purchase more tickets than would be available to a human user. *Id.* at 1155, 1175 & n.5. But Plaid offers no reason to believe that these sections of the CDAFA deviate from the CFAA in applying to damage to the integrity of computers and data because the substantive pleading standards for the CDAFA are the same as for the CFAA. *See Satmodo*, 2017 WL 6327132, at *7.

Plaintiffs adequately plead "intent to defraud" under the CFAA. Plaid argues that Plaintiffs'

[24] Plaid erroneously asserts that Plaintiffs do not allege facts showing it intended to cause damage under § 1030(a)(5)(A) or recklessly caused damage under § 1030(a)(5)(B). MTD at 27. Plaintiffs in fact have pleaded the requisite intent, and the case Plaid cites examined the evidence of Apple's intent in the context of a summary judgment motion. *See In re Apple & ATTM Antitrust Litig*, No. 07-5152, 2010 WL 3521965, at *7 (N.D. Cal. July 8, 2010).

claims under Sections 1030(a)(4) & (6) of the CFAA fail because they do not adequately allege Plaid intended to "deceive or cheat" (MTD at 28), but that is not the relevant legal standard. While the CFAA does not define "intent to defraud," courts in the Ninth Circuit have interpreted this phrase to mean proof of "unlawful access" or "wrongdoing," rather than to require proof of each of the elements of common law fraud. *See eBay Inc. v. Digital Point Solutions, Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009); *Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008). Intent can be shown where "the defendant participated in dishonest methods to obtain the plaintiff's secret information." *Shurgard*, 119 F. Supp. 2d at 1126.[25]

Plaintiffs adequately allege that Plaid acted with the requisite intent by alleging unlawful access and wrongdoing on Plaid's part. *See* ¶ 280 (Plaid accessed Plaintiffs' banks' computer systems "with the intent to collect banking data to which it was not entitled and which it intended to sell and use without authority"), ¶ 295 (Plaid transferred access tokens to the Apps "with the intent that those entities would use such access tokens or similar information to collect banking data to which they were not entitled, and that Plaid would be able to charge the Apps for the information or access"). Plaid cannot evade liability because it built its entire business around wrongful conduct. MTD at 28.

Plaid also is incorrect in asserting that "intent to defraud" under the CFAA is governed by Rule 9(b) pleading standards. *See NetApp, Inc. v. Nimble Storage*, 41 F. Supp. 3d 816, 833 (N.D. Cal. 2014) ("[M]ost CFAA cases in this district have not applied Rule 9(b)'s pleading standards to all CFAA claims."); *Facebook, Inc. v. MaxBounty*, 274 F.R.D. 279, 284 (N.D. Cal. 2011) ("fraud under the CFAA only requires a showing of unlawful access; there is no need to plead the elements of common law fraud") (quotation omitted). Even if Rule 9(b) applied to claims under Sections (a)(4) and (a)(6) of the CFAA, as discussed *infra* at Arg. § VI-F, Plaintiffs have adequately pleaded the who, what, when, where and how of Plaid's fraudulent actions.

Plaintiffs properly plead a claim under CFAA § 1030(a)(6). Plaid argues that Plaintiffs' allegations of trafficking under this provision are "conclusory" and "not supported by any facts at all." MTD at 28. But Plaintiffs' claim is amply supported by two alternative violations. ***First***, Plaid

[25] The case cited by Plaid, *Fidlar*, looked to inapposite Seventh Circuit authority interpreting "intent to defraud" in unnamed "similar statutes." 810 F.3d at 1079.

knowingly trafficked in "passwords or similar information through which a computer may be accessed" by obtaining "access tokens or similar information from Plaintiffs' and Class members' financial institutions through which the institutions' computer systems could be accessed without authorization." ¶ 293. ***Alternatively***, Plaid knowingly trafficked in passwords or similar information by "transferring to the Participating Apps access tokens or similar information from Plaintiffs' and Class members' banks through which the banks' computer systems could be accessed" using Plaid's software. ¶ 294. In both cases, Plaid's intent was to allow the Apps to access data from the banks. ¶¶ 293-94. In addition, Plaintiffs pleaded facts showing how such tokens or similar information are used in a typical "OAuth" process: "Behind the scenes, the bank returns a 'token' that allows the original app to access the consumer's bank information as necessary and authorized by the consumer, but without giving the app provider access to the login information." ¶ 33.

Plaintiffs thus allege facts showing that Plaid, using its "Managed OAuth" procedure, obtains access tokens or similar information that allow ongoing access to Plaintiffs' data stored at their banks, either directly from the banks (the first alternative scenario) or through Plaid (the second scenario). These factual allegations are clearly sufficient. *See Mobile Active Def., Inc. v. L.A. Unified Sch. Dist.*, No. 15-8762, 2016 WL 7444876, at *7 (C.D. Cal. Apr. 6, 2016) (allegation that the defendant provided another party a "secret, confidentially held URL" was sufficient under § 1030(a)(6) as transfer of information similar to a password). Plaid's challenge belongs at summary judgment.

Plaid also argues that Plaintiffs' allegations somehow contradict this claim, citing ¶ 68. MTD at 28. That argument fails because Plaintiffs allege that the language quoted in ¶ 68 is ***false and misleading***: "By stating that the login credentials will not be made accessible to Venmo, consumers are falsely led to reasonably expect that their credentials are not shared at all during the account verification process, other than with the bank they know and trust, while in fact those credentials are intercepted by Plaid for its use." ¶ 74(b). Plaid's receipt of an access token and transfer of that token to an App is fully consistent with these allegations. Also, Plaintiffs do not allege that Plaid trafficked in their login credentials, but rather in access tokens or similar information that Plaid received by using Plaintiffs' login credentials.

Because Plaintiffs allege that Plaid transferred the tokens or similar information to the Apps, the single case cited by Plaid is inapposite. *See Oracle Am., Inc. v. TERiX Comput. Co.*, No. 13-03385, 2014 WL 31344, at *6 (N.D. Cal. Jan. 3, 2014) ("Oracle has not alleged that Defendants transferred or otherwise disposed of its customer's login credentials. Instead, Defendants are alleged only to have received the login credentials from their customer and used the credentials themselves."); *see also T-Mobile USA, Inc. v. Terry*, 862 F. Supp. 2d 1121, 1131 (W.D. Wash. 2012) (upholding § 1030(a)(6) claim where the defendant and co-conspirators trafficked in "confidential pass-codes" that accessed "proprietary computer systems" and by trafficking in SIM cards which "operate[d] as a gateway (or computer password)" to a network); *NACM Tampa, Inc. v. Sunray Notices, Inc.*, No. 15-1776, 2017 WL 2209970, at *6 (M.D. Fla. Feb. 8, 2017) (upholding § 1030(a)(6) claim where the defendant transferred account and password information for the plaintiff's confidential database).

Plaintiffs properly plead claims under CFAA § 1030(a)(5)(A) and CDAFA § 502(c)(8). Plaid argues that these claims fail because Plaid's software is not like a virus or worm that "usurps the normal operation of the computer or computer system." MTD at 28-29. These statutes are not as limited as Plaid suggests. Plaid violated CFAA § 1030(a)(5)(A) by transmitting Plaintiffs' bank login information to access their banks' computer systems and by transmitting its software to the Apps for incorporation into their apps so that Plaid could collect Plaintiffs' login information, thereby causing damage to the banks' computer system and their data therein, as well as to Plaintiffs' smartphones and their data within. ¶¶ 283-84. Plaid argues that its software "does 'not impair the integrity or availability of' data or systems." MTD at 29 (quoting *Fidlar*, 810 F.3d at 1084). But the court in *Fidlar* recognized that the phrase "causes damage" in § 1030(a)(5)(A) ***both*** "encompasses clearly destructive behavior such as using a virus or worm or deleting data" ***and*** "may also include less obviously invasive conduct." *Id.* at 1084 (citation omitted). There is no basis for limiting a § 1030(a)(5)(A) claim as Plaid suggests.

Section 502(c)(8) of the CDAFA imposes liability upon one who "[k]nowingly introduces any computer contaminant into any computer, computer system, or computer network." Cal. Pen. Code § 502(c)(8). A "computer contaminant" is defined as "'***any*** set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer . . . without the intent or permission of the owner of the information.'" Cal. Pen. Code § 502(b)(10) (emphasis added). "The drafters spelled out that they intended this provision to encompass things ***including, but not***

limited to, 'a group of computer instructions commonly called viruses or worms.'" *Flextronics Int'l, Ltd. v. Parametric Tech. Corp.*, No. 13-00034, 2014 WL 2213910, at *6 (N.D. Cal. May 28, 2014) (quoting Cal. Pen. Code § 502(b)(10)) (emphasis added).

Plaintiffs allege that Plaid violated CDAFA § 502(c)(8) by knowingly introducing a computer contaminant into Plaintiffs' smartphones, in the form of the software it incorporated into the Apps to collect Plaintiffs' login information. ¶ 375. Plaid again argues, however, that its software does not "impair the integrity or availability of data or systems." MTD at 29. The court in *Flextronics* considered and rejected the same argument. *See* 2014 WL 2213910, at *6 ("PTC attempts to argue that because the technology does not 'usurp the normal operation of the computer,' it does not qualify as a 'contaminant.' However, that argument misinterprets an illustrative phrase at the end of a list of possible ways things that a set of computer instructions might do to be considered a 'contaminant.' Earlier in that same sentence, the statute teaches that a set of instructions which 'consume computer resources, modify, destroy, record, or transmit data' may also be considered a contaminant.") (quotation omitted).

Here, Plaintiffs have alleged sufficient facts showing that Plaid's software constitutes a set of instructions embedded in Plaintiffs' smartphones which record and transmit data. *See* ¶¶ 37-39, 45. Plaintiffs also sufficiently allege that Plaid's software was intended to damage the integrity of Plaintiffs' smartphones and their data therein. *See, e.g.,* ¶ 285(c). As a result, they have adequately alleged Plaid introduced a computer contaminant for purposes of their claim under § 502(c)(8).

D. <u>Plaintiffs Have Properly Pleaded A Claim Under The Stored Communications Act</u>

The SCA authorizes civil claims against anyone who intentionally accesses without or in excess of authorization "a facility through which an electronic communication service is provided" and thereby obtains or alters an electronic communication "while it is in electronic storage in such system . . . ." 18 U.S.C. §§ 2701(a), 2707. Plaid violated the SCA by accessing Plaintiffs' banks' computer systems without authorization, thereby obtaining access to the contents of Plaintiffs' electronic communications while they were in electronic storage. ¶ 307. To the extent Plaid obtained purported authorization to access those computers, it exceeded any authorization by collecting, aggregating, selling, and divulging the contents of electronic banking communications that were unrelated to the purpose for which Plaintiffs used the Apps. ¶ 308.

Plaid first argues that Plaintiffs' claims under the SCA fail because their banks do not constitute a "facility through which an electronic communication service is provided" because they are not an internet service provider, email provider, or bulletin board. MTD at 29. The SCA is not so restrictive. Contrary to Plaid's argument, Plaintiffs plausibly allege that each such entity's systems and servers constitute a facility under the SCA "which provides its users with the ability to send and receive electronic communications, including, *inter alia*, images, data, queries, messages, notifications, statements, forms, updates, and intelligence regarding the financial institutions and their policies and promotions, as well as about customers' individual accounts and activities, among others. ¶ 302 (citing 18 U.S.C. §§ 2701(a)(1); 2711(1), 2510(15) & 2510(12)). Plaintiffs further allege that their banks communicate information about their financial affairs, including "account balances, historical transactions, pending transactions, withdrawals, deposits, transfers, outgoing wires, loan terms, and interest rates through the electronic interface provided . . . for access via web browsers and the institutions' mobile apps." ¶ 302. *See Decoursey v. Sherwin-Williams Co.*, No. 19-02198, 2020 WL 1812266, at *6 (D. Kan. Apr. 9, 2020) (plaintiff adequately alleged that Facebook was a "facility" under the SCA, where she alleged that Facebook "provides its users with the ability to send and receive electronic messages"); *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 667 (D.N.J. 2013) (same) (citation omitted).

The cases Plaid cites are inapposite. *Central Bank & Trust v. Smith* is distinguishable because the bank at issue did not allege that the defendant accessed systems maintained by a third party that were designed for communication to consumers; rather, it alleged that former bank employees accessed its own servers and stole customer information to create a competing bank. 215 F. Supp. 3d 1226, 1234-35 (D. Wy. 2016); *accord Satcom Sol. & Res. LLC v. Pope*, No. 19- 02104, 2020 WL 4511773, at *6-7 (D. Colo. Apr. 20, 2020) (following *Central Bank* where former employee was alleged to have downloaded customer and marketing distribution lists to compete with former employer); *see also Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1041 (N.D. Cal. 2014) (under the SCA, "any 'facilities' must be operated by a third-party"). The other cases cited by Plaid have no application because Plaintiffs do not allege that their mobile devices constitute the facility at issue. *See In re iPhone Application*, 844 F. Supp. 2d at 1058 ("iOS devices do not constitute 'facilit[ies] through which an electronic communication service is provided'"); *Backhaut*, 74 F. Supp. 3d at 1041 ("mobile devices cannot be 'facilities'").

Plaid next argues that Plaintiffs failed to allege Plaid accessed an "electronic communication" in the form of "non-EFT information." MTD at 30. To the contrary, Plaintiffs alleged that Plaid accessed a host of "electronic communications," including (1) images, (2) data, (3) queries, (4) messages, (5) notifications, (6) statements, (7) forms, (8) updates, (9) intelligence regarding the financial institutions and their policies and promotions, (10) intelligence regarding their individual accounts and activities, and (11) information about their account balances, historical transactions, pending transactions, withdrawals, deposits, transfers, outgoing wires, loan terms, and interest rates. ¶¶ 302, 307; *see also* ¶ 56. Plaintiffs further allege that their banks store their "past banking activities, historical direct messages, and other communications." ¶ 305. As a result, the electronic communications at issue do not constitute "electronic funds transfer information" in the first place, and they are not stored "in a communications system used for the electronic storage and transfer of funds." 18 U.S.C. § 2510(12)(D).

Plaid also argues that Plaintiffs do not plausibly allege Plaid accessed a communication while it was in "electronic storage" because they do not allege that Plaid accessed any historical communications held "for purposes of backup protection." MTD at 30 (citing 18 U.S.C. § 2510(17)(B)). Plaid's argument fails because Plaintiffs have alleged facts showing that the communications at issue were stored, among other reasons, "for the purposes of backup protection," explaining that their banks "necessarily store historical communications regarding a customer's past banking activities, historical direct messages, and other communications so that they may be accessed by consumers, including Plaintiffs and Class members (*e.g.*, for tax purposes)." ¶ 305. Plaintiffs allege that Plaid accessed *all* information available at their respective banks, including such historical information held for backup purposes. *See, e.g.,* ¶ 56.

Contrary to Plaid's suggestion, courts recognize that information is held for backup purposes when it is stored in case the user needs to access and download it again, especially where data is made available for use outside the original system. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004) (emails remaining on NetGate's server after delivery were held for backup purposes should the user need to download them , such as if the emails were accidentally erased from the user's computer). The communications held by Plaintiffs' banks are fundamentally different than data that is only accessible through its place of storage and is not intended to be made available for use outside the original system. *See Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1044 (N.D. Cal. 2018) (distinguishing *Theofel* and finding that messages stored in a web-based email system were not held for purposes of backup protection because they were not meant to be downloaded outside of the original system); *United States v. Weaver*, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) (recognizing that where messages were downloaded to a different email client, the original system may hold messages for backup purposes). Here, Plaintiffs' banking information is useful outside of the bank's systems, which is why Plaid has built a business off retrieving that information from where it is maintained at the banks and delivering it elsewhere, updating that cache of data every few hours in the process. *See, e.g.*, ¶ 55.

Plaid also argues that Plaintiffs fail to allege that Plaid accessed data "without or in excess of authorization" or that it did so intentionally. The concept of authorization in the SCA is interpreted consistently with its interpretation under the CFAA. *See HiQ Labs*, 938 F.3d at 1002-03. Thus, for all the reasons discussed *supra* in Arg. § VI-C, Plaintiffs have properly alleged that Plaid acted without authorization or, alternatively, exceeded any purported authorization, in accessing Plaintiffs' banking data for purposes of their claims under the SCA.

Plaid argues, however, that because the SCA prohibits unauthorized access to information rather than use of that information, Plaintiffs' claims are somehow flawed. Plaid's argument misses the point. The cases Plaid cites distinguish between *access to* and *use of* data where the defendant was authorized to access the data in the first place, but then allegedly misused the data. *See, e.g., Central Bank*, 215 F. Supp. 3d at 1236 (SCA did not apply because the plaintiff did not allege "the defendants were accessing electronic information beyond what its information technology department authorized them to see").

To get around this obstacle, Plaid rehashes its same unsupported assertion that "[a]ny data Plaid allegedly *accessed* was accessed with Plaintiffs' authorization and at their request," attempting to conjure authorization from a mix of the terms of Plaid's privacy policy, the irrelevant client policies Plaid attaches to its counsel's declaration, and Plaintiffs' "stated purpose for using the apps." MTD at 31. For the reasons discussed *supra* at Arg. § II, Plaid's consent-based arguments are baseless.

E. <u>Plaid's Violations Of The California Anti-Phishing Act Are Well-Pled</u>

Plaid's violation of CAPA is clear: Plaid used the Internet to induce Plaintiffs to provide their financial account credentials and banking information ("identifying information," defined at Cal. Bus.

& Prof. Code § 22948.1) by representing itself to be Plaintiffs' financial institutions, without the institutions' authority or approval. *See* CAPA § 22948.2; ¶¶ 35, 38-41, 74(b)-(d), 321, 349-55; Facts § II. Holding Plaid responsible to the individuals whose unlawfully-obtained data it used to generate a windfall for itself is fully consistent with CAPA and the legislature's intent.

All elements of CAPA are well-pled. As an initial matter, Plaid does not dispute the well-pleaded allegations that it in fact used banks' logos and color schemes, or that the banking credentials and data it obtains are "identifying information" under CAPA. Instead, Plaid recycles its argument that despite Plaintiffs' detailed allegations showing Plaid hid the truth, consumers must have known anyway that they were not logging into their own banks (addressed *supra*, Arg. § II-A).

Plaid erroneously claims Plaintiffs do not support the allegation that Plaid acted "without obtaining the authority or approval of each financial institution" (MTD at 34; ¶ 353), but Plaintiffs specifically support their allegation with the fact that banks, and the ABA, voiced concerns about customer data acquisition by aggregators like Plaid (¶¶ 78-79); that banks compete with the Apps that use Plaid (¶ 81 n.65 & citation, describing "War Between Banks, Fintech Firms"); and that some of these banks took steps to stop Plaid from accessing their customers' data (¶¶ 80-81). In fact, and underscoring the adequacy of Plaintiffs' allegations, one institution, TD Bank, sued Plaid on October 14, 2020 for counterfeiting and unfair competition based on Plaid's use of TD's "trademarks, logo, and green color scheme to replicate TD's genuine login page and to dupe consumers into believing they are entering their sensitive personal and financial information in the bank's trusted and secure platform." Geman Decl. Ex. 1, at ¶ 4. Plaid is asking this Court to infer, improperly under the authority it cites,[26] that over 11,000 financial institutions (¶ 58)—one of which is now suing Plaid for this very conduct—actually authorized Plaid to acquire *their* customers' data by appropriating *their* branding, at the same time as they voiced concerns, competed with the fintech apps whose growth Plaid was facilitating, and tried to stop Plaid from accessing their customers' accounts. The CAC contradicts Plaid's argument, particularly drawn in a light most favorable to Plaintiffs.

[26] *See Bell Atlantic Corp. v. Twombly*, 550 U.S. 554, 555 (2007); *Ashcroft v. Iqbal* (2007), 556 U.S. 662, 678-80 (2009); *Adams v. Johnston*, 355 F.3d 1179, 1183 (9th Cir. 2004); *Johnson v. Riverside Healthcare Sys.*, 534 F.3d 1116, 1122 (9th Cir. 2008), cited by Plaid.

Plaintiffs were "adversely affected" by Plaid's phishing because Plaid acquired their private information under false pretenses. Plaintiffs thus have a statutory right to bring their claim for damages and the other relief. ¶¶ 253, 349-55; *supra* Facts §§ I-III; Arg. § III-B; CAPA § 22948.3(a)(2).

The law applies to Plaid. Plaid's primary argument asks the Court to ignore CAPA's plain text, declaring—without support—that the legislature must have intended to create an amorphous exception for "legitimate" businesses, which Plaid claims to be. MTD at 33. Absolutely nothing supports Plaid's contention. Both CAPA and its legislative history confirm that civil liability attaches to *any* entity that solicits private information by misrepresenting itself to be another business, as Plaid did. *See* CAPA § 22948.2 (unlawful for "*any*" person); Ex. 2 at 1 ("This bill makes it illegal for *anyone* to request that a consumer provide personal information by using e-mail, Web sites, or the Internet to impersonate a legitimate business.") (emphasis added). The statute does not limit who can be a defendant as Plaid suggests, or otherwise use "legitimate" or its synonyms. CAPA's history shows that lawmakers were concerned, *not* with insulating certain companies from liability, but with protecting "unsuspecting consumers" from providing personal information to false imitators of businesses—including banks specifically—whose reputations and customer relationships violators like Plaid exploit. *See* Ex. 3 at 1.[27]

Plaid's attempt to create an ill-defined exception, where CAPA itself is clear, violates basic canons of statutory interpretation. *See United States v. Neville*, 985 F.2d 992, 995 (9th Cir. 1993) ("[I]f the language of a statute is clear . . . then there is no need to 'interpret' the language by resorting to the legislative history or other extrinsic aids") (citation omitted). Judgments holding other established companies liable for their CAPA violations also give the lie to Plaid's position. *See, e.g. Facebook, Inc. v. Fisher,* No. 09-05842, 2011 WL 250395, at *2 (N.D. Cal. Jan. 26, 2011); *id.* ECF No. 1 (awarding injunction and statutory damages against otherwise legitimate marketing companies); *Greenwich Ins.*

[27] Earlier drafts of CAPA prohibited impersonating an "online business," but the language was amended to clarify that misrepresenting oneself as *any* business gave rise to a CAPA violation. *See* Ex. 3 at 4. For this reason, Plaid's assertion that the CAPA claim is a "red herring" because some banks do not have the technical capability to provide an OAuth protocol of their own (MTD at 7) is irrelevant—CAPA does not require a defendant to exactly replicate the businesses it impersonates. Indeed, liability does not even require that Plaid represented itself to "be" Plaintiffs' financial institutions (as it did), but could also be established with proof that Plaid purported to "represent" those institutions (as it also did). *See* Ex. 4 at 2 (to "indicate that he or she is or **represents** an online business without authorization from that business" would be an example of conduct violating CAPA) (emphasis added).

Co, v. Media Breakaway, LLC, No. 08-937, 2009 WL 6521581 (C.D. Cal. Jun. 11, 2009) (same, in arbitration).

CAPA must be broadly construed. Plaid is flat wrong to argue that the rule of lenity—under which penal statutes are construed strictly—exculpates Plaid from its scheme to pose as banks. MTD at 24 n.21, 33. CAPA is a *civil* statute in Business and Professions Code Division 8 (Special Business Regulations), not a penal statute, and it carries no criminal penalties. CAPA § 22948.3. "[T]he rule of strict construction of penal statutes" does not apply to civil statutes such as CAPA. *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 532 n.8 (2011). Instead, the California Supreme Court instructs that "courts should *liberally* construe remedial statutes in favor of their protective purpose." *Id.* (emphasis added). And, where lawmakers use broad language such as "any" (*e.g.*, "any person," "take any action" in CAPA § 22948.2), courts should infer that the legislature did not want the statutory protections to be narrowly construed. *See id.* at 533.

Certainly, Plaid's citations show that lawmakers were aware of criminal phishing schemes. MTD at 33; Ex. 3 at 3. However, as widely observed when CAPA came into force, California took a different approach from the criminal laws in certain other states, because of the legislature's interest in deterrence and use of civil liability as the appropriate vehicle to effectuate that purpose. *See* Camille Calman, *Bigger Phish to Fry: California's Anti-Phishing Statute and Its Potential Imposition of Secondary Liability on Internet Service Providers*, 13 Rich. J.L. & Tech. 2, 4 (2006); *see also* CAPA § 22948.3(d) (criminal remedies not *precluded* by statute). The bill's author's stated intent in introducing the law was to "improve the security of the Internet," and supporters of the law lauded its ability to preserve "confidence in the integrity of personal information transmitted via the internet [which is] an integral part of the medium's development." Ex. 3 at 3. Plaid's false banking login pages compromise confidence in financial technology apps precisely in the way that concerned the legislature and supporters of this law. *See, e.g.*, ¶ 79 (explaining that such practices create risk and undermine consumer trust).

Accordingly, contrary to Plaid's suggestion (MTD at 34), this remedial statute does not require Plaintiffs to plead that Plaid's "goal" was to commit identity theft. *See* CAPA § 22948.2; Ex. 7 at 2 (explaining CAPA would change "existing law," which required proving intent to defraud). Even if it did, Plaintiffs plainly allege that Plaid's purpose in violating CAPA was to acquire banking credentials for classic identity theft, *i.e.*, to pose as consumers logging into their financial accounts in order to extract their banking data. *See* ¶ 40 (Plaid's interface was designed "for the purpose of ensuring . . . its process would fool consumers" into "handing their login information to a third party."); ¶ 32 ("Plaid has achieved its success by accessing all of the data stored in consumers' financial accounts without consumers' knowledge or consent."); ¶ 27 ("Plaid's true purpose is to monetize consumer transactional and other banking data"); ¶¶ 29, 34, 39, 41, 45, 46, 48-58.

F. <u>Plaintiffs Properly Plead A Claim For Deceit</u>

Plaid argues in error that Plaintiffs cannot meet any of the five elements for deceit under California law. MTD at 34. Plaintiffs plead facts supporting each element with the requisite specificity.

First, Plaid concealed and failed to disclose its true nature and conduct through misleading statements, omissions, and nondisclosures. ¶¶ 360(a)-(f). As discussed *supra* at Arg. § II, Plaid cannot defeat these well-pled allegations by trotting out its privacy policy.

Second, Plaid had a duty to disclose. Deceit is not limited to fiduciary relationships, but extends to where "the defendant [has] excusive knowledge of material facts not known to the plaintiff", where there is "active conceal[ment of] a material fact", or where "the defendant makes [a] partial representation[] but also suppresses some material facts." *Hoffman v. 162 N. Wolfe LLC*, 228 Cal. App. 4th 1178, 1187 (2014), *as modified* (Aug. 13, 2014). In such alternatives, "[a] relationship between the parties is present if there is 'some sort of *transaction* between the parties.' . . . like any kind of contractual agreement." *Id.* (emphasis in original). Plaintiffs allege they were involved with transactions with Plaid (albeit unbeknownst to them) whereby they connected the Apps to their bank accounts using Plaid's software that was embedded in the Apps, unwittingly granting Plaid the keys to their accounts (and access to all the data therein) in the process. *See* ¶¶ 100-207. Those transactions create the minimal relationship required for Plaid to have a duty to disclose arising out of its exclusive knowledge of material facts not known to Plaintiffs (¶ 360(a), (c)), its active concealment of material facts (¶ 360(d)), and its partial representations while suppressing some material facts. ¶ 360(b), (e)-(f).

Third, Plaid's deceit was intentional. Intent may be alleged generally, Fed. R. Civ. P. 9(b), and there are more than sufficient allegations in the CAC. *See, e.g.*, ¶¶ 40-41, 76-77. Again, Plaid's only rebuttal is to point to its legally (and factually) insufficient privacy policy, which was so dramatically minimized in the account linking process, and is drafted so broadly and misleadingly, that the policy in itself suggests an intent to deceive. *See supra* Arg. § II.

Fourth, Plaintiffs adequately plead reliance. In an omissions case such as this, reliance may be shown by showing that "had the omitted information been disclosed, [the plaintiff] would have been aware of it and behaved differently." *Sloan v. GM, LLC*, 287 F. Supp. 3d 840, 873 (N.D. Cal. 2018) (quotation omitted). This "can be presumed, or at least inferred, when the omission is material." *Id.* at 874. A misrepresentation is material "if a reasonable man [*sic*] would attach importance to its existence or nonexistence in determining his choice of action in the transaction in question"—"as such materiality is generally a question of fact." *Id.* (quotation omitted); *see also Hoffman*, 228 Cal. App. 4th at 1193-94 (reliance is a factual issue that may only be decided as a matter of law "if reasonable minds can come to only one conclusion based on the facts," and then only on summary judgment).[28] At the pleading stage, it suffices for Plaintiffs to allege that they would not have entered the transaction if they had been aware of the omitted information. *See Sloan*, 287 F. Supp. 3d at 874. Plaintiffs have pled just that. ¶¶ 105, 116, 126, 135, 145, 155, 164, 173, 183, 194, 204.[29]

Fifth, Plaid argues that Plaintiffs fail to allege damage, cross-referencing the arguments it made regarding injury-in-fact. MTD at 36. For the reasons stated *supra* at Facts § III and Arg. §§ III-A, C & D, Plaid's argument fails.

Sixth, Plaintiffs satisfy Rule 9(b). Particularity can be met, as it is here, by Plaintiffs' description of what is misleading about a webpage or other online content that is "specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud." *Ferrington v. McAfee, Inc.*, No. 10-01455, 2010 WL 3910169, at *2, *6 (N.D. Cal. Oct. 5, 2010) (quotation omitted) (9(b) satisfied by describing misleading aspects of a pop-up ad, including how it mimicked the look of other pages, the ad's contents, and the color and font of information in the ad). Likewise, Plaintiffs plead

[28] That Plaid's violations implicate the GLBA, which requires privacy notices to be "clear and conspicuous," further underscores the materiality of the omitted information. Consumers must have meaningful choice in connection with their sensitive financial information.

[29] Plaid also improperly relies on its privacy policy as a defense against the well-pleaded allegations of reliance (MTD at 36).

the specific misconduct that is fraudulent, including misleading statements and omissions in Plaid's template software (along with the font size, color, lack of underlining, and other elements of the screens at issue), as well as misleading statements and omissions in its privacy policy. ¶¶ 37-39, 66-75. Plaid is on notice as required by Rule 9(b).

Plaid cites a different and non-governing articulation of 9(b) as set forth in *Marolda v. Symantec Corp.*, 672 F. Supp. 2d 992 (N.D. Cal. 2009), but that case is distinguishable and its holding has not been adopted. *See, e.g., Overton v. Bird Brain, Inc.*, No. 11-1054, 2012 WL 909295, at *6 (C.D. Cal. Mar. 15, 2012) ("[T]he *Marolda* requirements are not necessarily appropriate for all cases alleging a fraudulent omission."). Nevertheless, Plaintiffs have satisfied even this non-applicable standard as well by providing "representative samples" of the screens Plaid employed. *See* ¶¶ 38, 67 (sample screens from Venmo and Plaid's bank login templates).

G. Plaintiffs State A Claim For Unjust Enrichment/Quasi-Contract

Plaintiffs state a claim for unjust enrichment/quasi-contract, entitling them to restitution of the economic benefits Plaid gained by violating their rights. Plaid's argument about remedies at law is addressed *supra*, Arg. § V. Plaid is incorrect to argue that California does not recognize this claim. *Astiana*, 783 F.3d at 762 (unjust enrichment a claim); *see also Brazil v. Dole Packaged Foods, LLC*, 660 F. App'x 531, 535 (9th Cir. 2016) (reversing district court's dismissal of a claim for unjust enrichment); *In re Vizio*, 238 F. Supp. 3d at 1233 (C.D. Cal. 2017); *Trazo v. Nestle USA, Inc.*, 113 F. Supp. 3d 1047, 1049 (N.D. Cal. 2015) (citing *Astiana* and reinstating plaintiff's quasi-contract claims). Plaid's only case, *McLellan v. Fitbit, Inc.*, fails to advert to *Astiana* or other binding law and references unjust enrichment in one conclusory sentence. No. 16-00036, 2018 WL 2688781, at *4 (N.D. Cal. June 5, 2018).

To the extent Plaid takes issue with the sufficiency of its alleged "misrepresentation or omission" (MTD at 37), this is addressed in previous sections, and belied by the robust allegations in the CAC. *See, e.g.*, ¶¶ 74, 76, 229 (summarizing the "unethical, unfair, and deceptive practices Plaid employed); *supra*, Facts § I and Arg. §§ VI-B & F. Plaid unjustly retained the meaningful monetary benefits of harvesting and selling Plaintiffs' data. ¶¶ 6, 62-63, 229, 320-24, 333, 354. These allegations far exceed the "straightforward statement" required to state this cause of action. *Astiana*, 783 F.3d at 762-63.

CONCLUSION

For all the foregoing reasons, Plaintiffs respectfully request that the Court deny Plaid's Motion to Dismiss and allow this case to proceed on the merits. In the alternative, the Court should grant leave to amend. Contrary to Plaid's assertions that Plaintiffs have amended five complaints with "ample time" (MTD at 2, 38), Interim Co-Lead Class Counsel have filed one consolidated complaint in this action, on August 5, 2020, seven days after they were appointed. Dkt. 57. The sufficiency of that pleading has not previously been addressed. *See U.S. v. United Healthcare Ins. Co.*, 848 F.3d 1161, 1183 (9th Cir. 2016); *Moss v. U.S. Secret Serv.*, 572 F.3d 962, 972 (9th Cir. 2009) ("requests for leave should be granted with 'extreme liberality'") (citation omitted).

Dated: November 17, 2020

HERRERA PURDY LLP

/s/ Shawn Kennedy
Shawn M. Kennedy

Shawn M. Kennedy (SBN 218472)
skennedy@herrerapurdy.com
Andrew M. Purdy (SBN 261912)
apurdy@herrerapurdy.com
Bret D. Hembd (SBN 272826)
bhembd@herrerapurdy.com
4590 MacArthur Blvd., Suite 500
Newport Beach, CA 92660
Tel: (949) 936-0900
Fax: (855) 969-2050

HERRERA PURDY LLP
Nicomedes Sy Herrera (SBN 275332)
nherrera@herrerapurdy.com
Laura E. Seidl (SBN 269891)
lseidl@herrerapurdy.com
1300 Clay Street, Suite 600
Oakland, CA 94612
Tel: (510) 422-4700
Fax: (855) 969-2050

Dated: November 17, 2020

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

/s/ Rachel Geman
Rachel Geman

Rachel Geman (*Pro Hac Vice*)
rgeman@lchb.com
Rhea Ghosh (*Pro Hac Vice*)
rghosh@lchb.com
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Tel: (212) 355-9500
Fax: (212) 355-9592

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol (SBN 194857)
msobol@lchb.com
Melissa Gardner (SBN 289096)
mgardner@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel: (415) 956-1000
Fax: (415) 956-1008

Dated: November 17, 2020

BURNS CHAREST LLP

/s/ Christopher Cormier
Christopher J. Cormier

Christopher J. Cormier (*Pro Hac Vice*)
ccormier@burnscharest.com
4725 Wisconsin Avenue, NW
Washington, DC 20016
Tel: (202) 577-3977
Fax: (469) 444-5002

BURNS CHAREST LLP
Warren T. Burns (*Pro Hac Vice*)
wburns@burnscharest.com
Russell Herman (*Pro Hac Vice*)
rherman@burnscharest.com
900 Jackson Street, Suite 500
Dallas, TX 75202
Tel: (469) 904-4550
Fax: (469) 444-5002

Interim Co-Lead Class Counsel